H3C网络学院参考书系列

H3C



收藏的是情怀
学习的是技术
解决的是问题

总裁推荐
典藏版
双色精装

根叔的云图

——网络故障大排查

杭州华三通信技术有限公司　编著

清華大学出版社

根叔的云图

——网络故障大排查

杭州华三通信技术有限公司　编著

清华大学出版社
北　京

内 容 简 介

本书是新华三集团一百多位专家基于自身十多年的故障定位经验而编写的，给出了大量典型故障的定位思路，技术涵盖网络技术、云计算、服务器等，产品覆盖了路由器、交换机、安全产品、无线产品、iMC 管理软件、云计算产品、服务器、EPON 等。

本书是为具备一定 IP 网络基础知识的人员编写的，尤其适合于学习了 H3C 网络学院系列教程的读者。对于 IT 技术人员，本书是简单易用的 H3C 产品故障排查手册，另外本书还可以作为 H3C 网络学院系列教程的补充教材。

图书在版编目(CIP)数据

根叔的云图：网络故障大排查/杭州华三通信技术有限公司编著. —北京：清华大学出版社，2016
（H3C 网络学院参考书系列）
ISBN 978-7-302-45379-6

Ⅰ. ①根…　Ⅱ. ①杭…　Ⅲ. ①计算机网络—故障修复　Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字(2016)第 254425 号

责任编辑：田在儒
封面设计：牟兵营
责任校对：李　梅　袁　芳
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　**邮　　编**：100084
社 总 机：010-62770175　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市中晟雅豪印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　**印　　张**：84.25　**字　　数**：2154 千字
版　　次：2016 年 12 月第 1 版　**印　　次**：2016 年 12 月第1 次印刷
印　　数：1～2000
定　　价：498.00 元

产品编号：066350-01

本书编委会

主　　编　邹双根

副 主 编　张东亮　马文斌　秦　军　程　飞　苇启跃　余　晨　何　颖　寻尚岩　厉梦如　徐　浩

参编人员　（以下按姓氏笔画排序）

丁　犁　马文斌　马光彬　马　昊　马鹏飞　王　京
王树旺　王剑虎　王　锐　孔天娇　厉梦如　丘岳维
付　睿　白靖宁　吕扬然　朱玉广　向健民　刘林涛
关　萌　寻尚岩　纪合宝　孙培浩　杜奕山　杨　勇
杨银波　李长剑　李晨光　酉海华　肖　李　肖春喜
吴骋骐　何　理　余　晨　邹　鹏　沈博文　张　辛
张　玺　张　磊　陈丹威　陈　宇　陈明槐　陈　铮
罗　旭　金　山　周振华　赵　杰　赵国卫　赵　跃
郝云龙　洪黔华　费　腾　秦　军　苇启跃　徐　浩
高贵贤　唐　斌　梅　青　常　衫　彭绍穗　程　飞
舒中华　解麟猛　翟运波　樊　昊

版权声明

H3C 网络学院参考书系列

《根叔的云图——网络故障大排查》
(V1.0)

杭州华三通信技术有限公司编著

2016 年 11 月印刷

序

新一轮科技革命方兴未艾，不断推陈出新的信息技术（IT）正越来越迅速地、深刻地影响着人们的工作与生活。IT正重新塑造并雕琢着社会经济的整体全貌与细节，将人类社会带入了一个全新的时代。

新华三集团，作为IT产业的一员，时刻站在科技研发与推进IT发展的前沿，将最新的信息技术创新地应用于各行业实践，为这个全新的时代做出自己的贡献。随着新华三集团的产品和解决方案不断地应用于“百行百业”，新华三也积累了越来越多的具有示范效应的行业最佳实践，形成了一大批被业界喻为“教科书”般的优秀应用案例。我相信，您使用的每一次信息服务都可能有新华三集团在背后默默的支持。

作为有影响力、有社会担当的IT企业，我们有责任和义务将新华三的成熟经验推广到全社会，为信息化建设做出自己的贡献，履行自己的社会责任。在合作伙伴、客户、高校及广大IT爱好者的建议与要求下，我们通过新华三集团下属的新华三大学将这些实践智慧与宝贵经验汇集成书，正式出版，与众共享，让全社会都能分享到新华三专家十多年的智慧成果，为我国的IT人才培养与IT实践发展诚尽一份心力。

《根叔的云图——网络故障大排查》就是这一系列分享的第一本书，也可能是目前业界唯一一本网络运维操作宝典。该书采用了新颖、独创的“云图”方式，将非常复杂的IT运维技术总结成思维导图，以清晰、富有逻辑、易于掌握的方式呈现出来，把复杂的事情简单化，给技术人员“授人以渔”。

在此，我寄望广大读者能从本书中感受到新华三众多技术专家对技术前沿的天生痴迷、对应用实践的倾情投入；感受到每一位新华三人对于通过技术创新与精准服务，进而推动百行百业不断发展的热望与执着；感受到新华三作为中国IT领军企业，为整个IT产业的发展、社会经济的进步所付出的不懈努力！

新华三集团总裁兼首席执行官

2016年11月于北京

前　　言

随着互联网技术的广泛普及和应用，通信及电子信息产业在全球迅猛发展起来，从而也带来了网络技术人才需求量的不断增加，网络技术教育和人才培养成为高等院校一项重要的战略任务。

H3C 网络学院（HNC）主要面向高校在校学生开展网络技术培训，培训使用 H3C 网络学院培训教程。HNC 教程包括《中小型网络构建与维护》《路由交换技术》《IPv6 技术》等。培训课程高度强调实用性和提高学生动手操作的能力。

作为 H3C 网络学院课程的参考书，《根叔的云图——网络故障大排查》侧重于对学生网络故障排查能力的培养。本书适合以下几类读者。

IT 技术人员：本书能够使 IT 技术人员根据故障现象快速排查 H3C 设备故障。

职业院校在校学生：本书可作为 H3C 网络学院课程的教学辅助教材，也可作为 IT 相关专业学生的自学参考书。

IT 技术爱好者：本书可以作为所有对 IT 技术感兴趣的爱好者学习 IT 技术、提高故障排查能力的自学参考书籍。

本书主要以贴近实际网络的动手实验为主，内容由浅入深，配合通俗易懂深入浅出的知识介绍。这充分突显了 H3C 网络学院系列教程的特点——专业务实、学以致用。本书经过精心设计，便于知识的连贯和理解，学员可以在较短的学时内完成全部内容的学习。本书所有内容都遵循国际标准，从而保证了良好的开放性和兼容性。

全书共 10 章。

第 1 章　公共协议

本章介绍了公共协议的故障排查思路，包括静态路由、RIPv2、OSPF、BGP、IGMP、MPLS VPN、MSTP、RSTP 等。

第 2 章　路由技术

本章介绍了路由相关技术的故障排查思路，包括串口、E1 接口、3G 接口等接口故障排查，包括 DHCP、NAT 等 IP 业务故障排查，包括 PPP、HDLC、DCC、FR 等广域网接入技术故障排查，包括 GRE、L2TP、DVPN 等 VPN 故障排查，包括 AM、FCM、E1POS 等终端接入故障排查，以及 QoS、VoIP 等故障排查。

第 3 章　交换技术

本章介绍了交换相关技术的故障排查思路，包括以太网链路、以太网接口、QinQ、BPDU Tunel、Voice VLAN 等以太网二层技术故障排查，包括端口安全、Portal 认证、MAC 地址认证等安全接入故障排查，包括 VRRP、Track、RRPP 等可靠性故障排查以及 QoS、Radius、TACACS 等故障排查。

第 4 章　路由器产品

本章介绍了路由器产品相关故障的排查思路，包括 MSR G2 设备 License 异常故障排查、MSR 风扇故障排查、PPPoE client 故障排查、PPPoE server 故障排查、CR16000 和 SR8800 产

品硬件故障排查、MSR硬件故障排查、MPLS L2VPN(V7)故障排查、配置策略路由后业务不通故障排查、等价路由不能达到负载效果故障排查、内网用户无法通过域名访问内部服务器故障排查、SR66系列路由器电源模块故障排查、SR66设备硬件故障排查、ER系列路由器掉线故障排查、ER系列路由器忘记密码故障排查等。

第5章 交换机产品

本章介绍了交换机产品相关故障的排查思路,包括高端产品电源故障排查、高端产品业务板CPU利用率高故障排查、高端产品转发丢包故障排查、高端产品IRF2堆叠无法建立故障排查、高端产品板卡无法注册故障排查、S12500/S9500E产品风扇故障排查、S12500/S9500E产品镜像组无法下发故障排查、高端交换机策略路由不生效问题排查、CR16000/SR8800产品风扇故障排查、Smart Link故障排查、VLAN MAPPING故障排查、常见盒式交换机硬件故障排查、高端交换机等价路由及链路聚合出口流量负载不均故障排查、高端交换机二次电源故障排查、常见框式交换机硬件故障排查、12500_9500E端口镜像不生效故障排查、中低端交换机(V5)光口不能Up故障排查、PoE故障排查、高端交换机MQC重定向不生效故障排查、中低端交换机(V5)等价路由出口流量负载不均故障排查、无管理交换机转发异常故障排查、AGMP管理类故障排查、SMB交换机掉线故障排查、SMB交换机配合应用软件使用故障排查、SMB可管理交换机忘记密码故障排查、ARP-DETECTION故障排查、中低端设备CPU利用率高故障排查等。

第6章 安全产品

本章介绍了安全产品相关故障的排查思路,包括IPSec VPN故障排查、PKI故障排查、OAA故障排查、SSH故障排查、SSL VPN故障排查、公钥管理故障排查、ACG1000微信认证故障排查、ACG1000应用审计功能故障排查、ACG1000 URL功能问题故障排查、ACG1000日志功能故障排查、防火墙CPU利用率高故障排查、防火墙NAT故障排查、防火墙Web网管故障排查、防火墙丢包故障排查、防火墙内存利用率高故障排查、防火墙双机热备故障排查、防火墙域间策略故障排查、防火墙重启故障排查、防火墙链路聚合故障排查、防火墙攻击防范故障排查、防火墙ALG故障排查、M9000丢包问题故障排查、M9000内存高问题故障排查、IPS防病毒功能故障排查、IPS防攻击功能故障排查、M9000 CPU利用率高故障排查、M9000 NAT功能故障排查、M9000版本升降级故障排查、M9000日志功能故障排查、LB NAT方式服务器负载均衡故障排查、LB Outbound链路负载均衡故障排查、LB健康性检测故障排查、LB Inbound链路负载均衡故障排查、LB DR方式服务器负载故障排查、IPS(ACG)MQC引流问题故障排查、IPS(ACG)URL过滤功能故障排查、IPS(ACG)Web登录故障排查、IPS(ACG)带宽管理功能故障排查、IPS(ACG)日志功能故障排查、IPS(ACG)上网慢故障排查等。

第7章 无线产品

本章介绍了无线产品相关故障的排查思路,包括无线设备CPU利用率高故障排查、无线设备内存利用率高故障排查、AC异常重启故障排查、网管采集无线设备数据异常故障排查、无线AC CAPWAP备份故障排查、无线组播故障排查与优化、无线AC PSK认证故障排查、AC Portal热备故障排查、无线AC硬件故障排查、无线AC静态路由故障排查、DHCP Server故障排查、无线指纹定位故障排查、VRRP+NQA联动失败故障排查、室外无线CPE应用网速慢、体验差故障排查、无线CUPID定位故障排查、无线非WLAN干扰故障排查、无线控制器VRRP故障排查、瘦AP注册不上故障排查、本地转发异常故障排查、无线桥接故障排查、无线X分信号覆盖不佳故障排查、无线桥接快速切换故障排查、无线终端硬件故障排查、无线

终端丢包问题定位故障排查、无线终端关联失败故障排查、MAC 接入认证故障排查、本地 Portal Server 故障排查、无线 MAC 快速认证故障排查、无线 Portal 认证故障排查、移动 WLAN 话单故障排查、无线 PSK 认证故障排查、VRRP＋NQA 联动失败故障排查、无线 802.1x 认证故障排查等。

第 8 章　iMC 管理软件

本章介绍了 iMC 管理软件相关故障的排查思路，包括 iMC 安装部署故障排查、iMC 设备管理故障排查、iMC 告警管理故障排查、iMC License 故障排查、iMC Dbman 备份故障排查、iMC 性能管理故障排查、iMC 拓扑管理故障排查、Portal 认证页面无法弹出故障排查、Portal 无感知认证故障排查、iMC 数据库故障排查、iNode 安装运行故障排查、WSM 无法识别或同步 AC 故障排查、拓扑常见问题排查、防破解故障排查、备份设备配置文件失败故障排查、iMC 页面显示乱码故障排查、iMC 页面响应慢故障排查、访客二维码认证故障排查、WSM 射频管理故障排查、iMC APM 数据库管理故障排查、防内网外连故障排查、访客基本功能故障排查、iMC NTA/UBA 管理 NetStream 日志故障排查、iMC UBA 管理 NAT 及 FLOW 日志故障排查、802.1x 认证故障排查、UAM Portal 认证故障排查、LDAP 用户管理故障排查、证书认证故障排查、EIA 之 BYOD 特性故障排查、EAD 补丁管理故障排查、EAD 防病毒软件故障排查、WSM 资源管理故障排查、桌面资产管理故障排查、DAM 软件分发故障排查、EAD 可控软件管理故障排查、iMC BIMS 组件问题分析、APM 应用监控故障排查、iMC 双机冷备方案故障排查等。

第 9 章　云计算产品

本章介绍了云计算产品相关故障的排查思路，包括 H3C CAS 云计算平台 License 使用、虚拟机启动异常故障排查、零存储集群添加节点异常问题排查、H3C CAS 云计算平台虚拟机优化、DRX 业务扩展故障排查、虚拟机手动迁移失败故障排查、FlexServer R390 服务器指示灯告警故障排查、刀片服务器开机故障排查等。

第 10 章　EPON_EoC 产品

本章介绍了 EPON_EoC 产品相关故障的排查思路，包括 ONU 注册类故障排查、ONU 长发光故障排查、OLT 上无法 ping 通 ONU 的管理地址故障排查、SMB V5 交换机 POE 故障排查、EoC 双向网改造导致电视播放异常故障排查、EoC 头端无法管理故障排查、EoC 网络 PPPoE 拨号上网故障排查、EoC 终端注册不上故障排查、EoC 终端配置下不生效故障排查等。

由于编者水平有限，书中难免有疏漏之处，敬请读者批评指正。

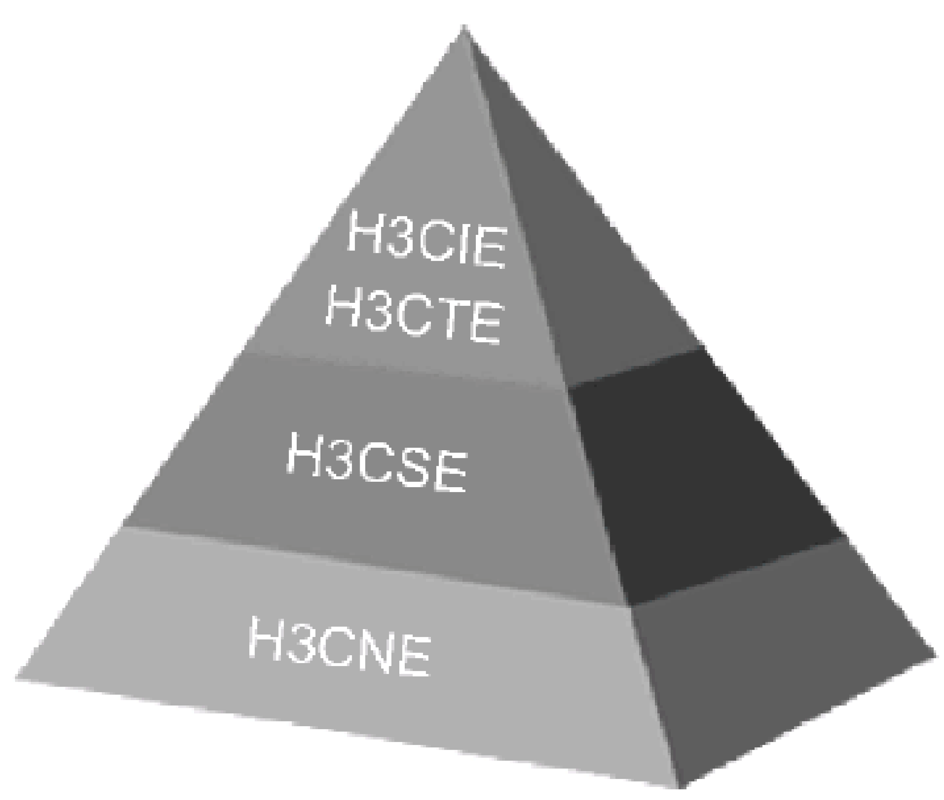
新华三大学培训开发委员会
2016 年 11 月

目　　录

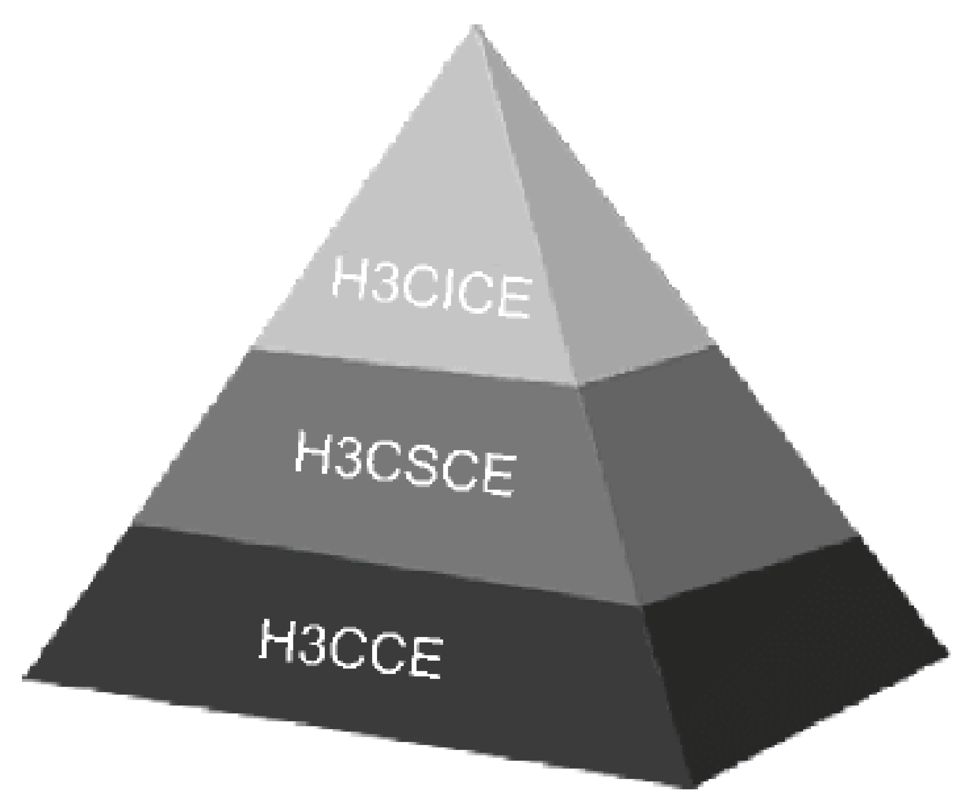
H3C 认证简介

H3C 认证培训体系是中国第一家建立国际规范的完整的网络技术认证体系，H3C 认证是中国第一个走向国际市场的 IT 厂商认证。H3C 致力于行业的长期增长，通过培训实现知识转移，着力培养高业绩的缔造者。目前在全球拥有 20 余家授权培训中心和 380 余家网络学院。截止 2014 年底，已有 40 多个国家和地区的 23 万余人次接受过培训，逾 12 万人次获得认证证书。H3C 认证将秉承“专业务实，学以致用”的理念，快速响应客户需求的变化，提供丰富的标准化培训认证方案及定制化培训解决方案，帮助您实现梦想、制胜未来。

按照技术应用场合的不同，同时充分考虑客户不同层次的需求，H3C 公司为客户提供了从网络助理工程师到网络专家的四级网络认证体系和应运而生的云计算认证体系。



网络认证体系



云计算认证体系

H3C 认证将秉承“专业务实，学以致用”的理念，与各行各业建立更紧密的合作关系，认真研究各类客户不同层次的需求，不断完善认证体系，提升认证的含金量，使 H3C 认证能有效证明您所具备的网络技术知识和实践技能，帮助您在竞争激烈的职业生涯中保持强有力的竞争实力！

新华三大史记·根叔列传

根叔，东吴人士，年近四旬，H3C TAC 中心资深工程师。沉浸“攻城之术”二十载有余，颇有心得。深感众工程师“日夜劳作，披星戴月，早起于鸡，晚睡于狗，常呕心沥血，或命悬一线”。思之：吾生也有涯，而城池亦有涯。诸城或大或小，或产品或协议，或固若金汤，或坚如磐石，恰如世间万物，皆暗合天数，有迹可循。后每下一“城”，则做图一卷，绘该城之奥妙，剖机关之精巧。日后若再攻此“城”，则按前图索骥。故一触即溃，城危如累卵。若遇图不能穷尽之处，则修改之，增益之，日渐精进。日积月累，共得图两百余卷，卷卷彩绘于锦帛之上，琉璃璀璨，美若云裳。自命为：云图。视为珍宝，藏于隐秘之处。若他人求见，则怒斥：吾之命根，岂肯轻易示人！日久，众皆称其为：根叔。

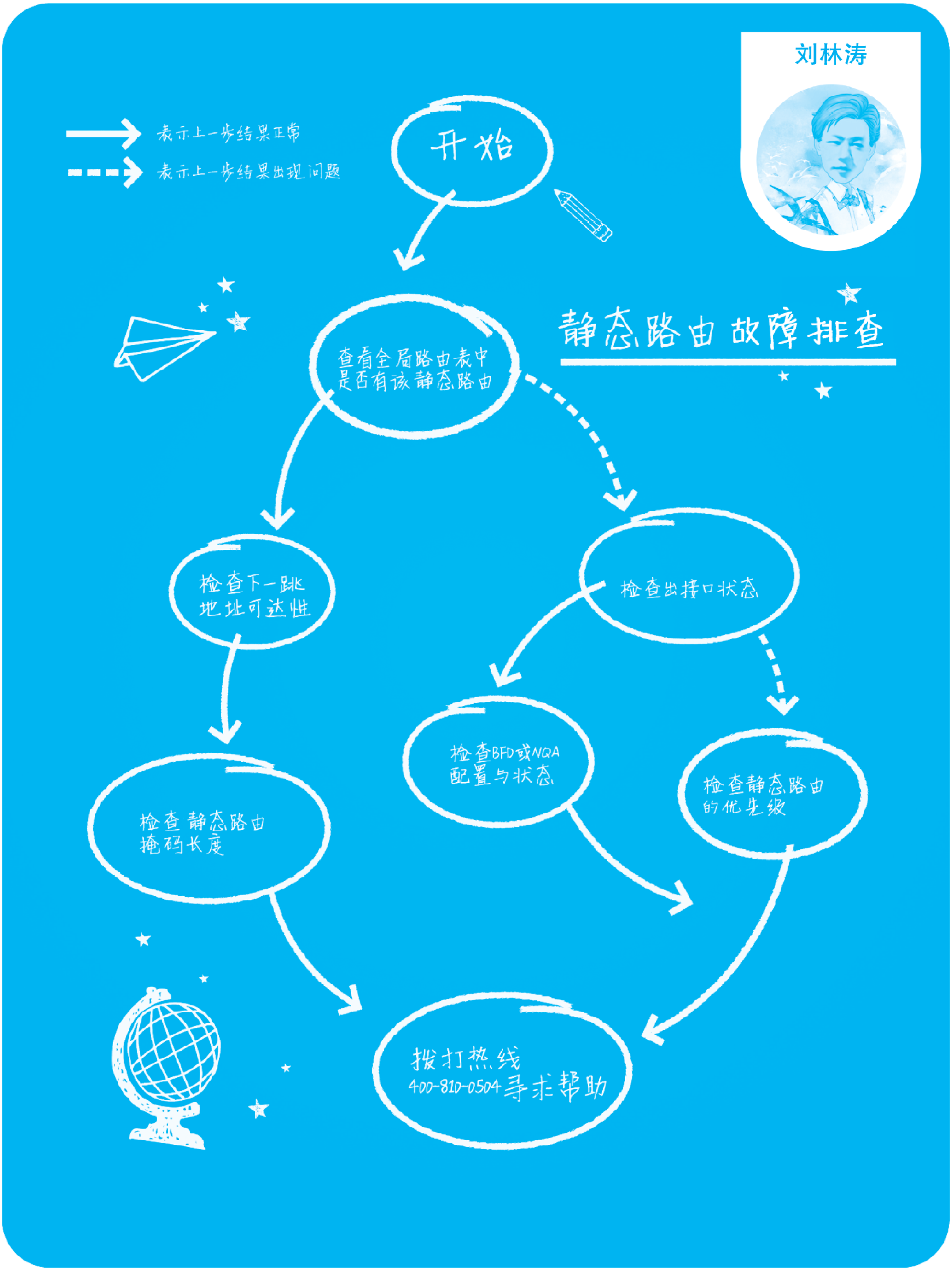
根叔近年自觉年事已高，恐日后登梯攻城时误中流矢，则云图宝典永无见天日矣。纠结数月，某日顿悟：愿将绝学公之于众，愿救众工程师于水火。

IT 江湖得知，一片哗然，众帮派掌门及其小伙伴皆惊矣，叹曰：古有《孙子兵法》一十三篇，今有根叔云图两百余卷！将本帮安身立命之绝学造福天下者，前未尝闻也。H3C TAC 中心，高端、大气、上档次！

李劲松

01

公共协议


刘林涛
表示上一步结果正常
表示上一步结果出现问题
开始
静态路由故障排查
查看全局路由表中是否有该静态路由
检查下一跳地址可达性
检查出接口状态
检查BFD或NQA配置与状态
检查静态路由掩码长度
检查静态路由的优先级
拨打热线400-810-0504寻求帮助

01 公共协议 > 1.1 IP 路由 > 1.1.1 静态路由故障排查 > 步骤详解

1. 开始

静态路由是否能够加入到全局路由表中并成功指导报文正确转发，取决于其出接口状态与下一跳地址可达性，以及相关检测联动的状态等方面。因此静态路由定位故障的思路是：首先查看全局路由表中是否有该静态路由；然后据此相应地检查出接口状态、下一跳地址可达性、BFD/NQA 配置、路由优先级等。

2. 流程图相关操作说明

(1) 查看全局路由表中是否有该静态路由

命令：*display ip routing-table xxx.xxx.xxx.xxx*(目的 IP 网段)

例如：通过上述命令查看，可以确认全局路由表中存在该静态路由。

```
<H3C>display ip routing-table 192.168.2.0
Routing Tables: Public
          Destinations : 1          Routes : 1
Destination/Mask      Proto   Pre   Cost      NextHop        Interface
192.168.2.0/24        Static  60    0         192.168.1.2    GE0/0
```

(2) 检查出接口状态

查看静态路由对应的出接口状态是否正常，正常情况下该接口的物理层状态、协议层状态均为 Up。接口状态问题参见接口排错。

命令：*display interface brief*

例如：通过上述命令查看，可以确认出接口的物理层和协议层状态均正常。

```
<H3C>display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link    Protocol    Main IP          Description
Eth6/0             Down    Down        --
GE0/0              Up      Up          192.168.1.1
```

(3) 检查下一跳地址可达性

查看静态路由下一跳地址，验证其是否可达。

命令：*display ip routing-table protocol static xxx.xxx.xxx.xxx*(目的 IP 网段)

pingxxx.xxx.xxx.xxx(下一跳 IP 地址)

例如：通过上述命令，可以确认静态路由下一跳地址可达。

```
<H3C>display ip routing-table protocol static 192.168.2.0
...
Static Routing Table Status : <Active>
Summary Count :1
```

```
Destination/Mask    Proto    Pre  Cost    NextHop        Interface
192.168.2.0/24      Static   60   0       192.168.1.2    GE0/0

<H3C>ping 192.168.1.2
PING 192.168.1.2: 56   data bytes, press CTRL_C to break
    Reply from 192.168.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    …
```

（4）查看是否绑定 BFD 或 NQA

查看静态路由是否绑定了 BFD 或 NQA，与 BFD 或 NQA 检测进行联动。

命令：*display current-configuration* ｜ *include xxx.xxx.xxx.xxx*（目的 IP 网段）

例如：通过上述命令查看，可以确认静态路由绑定了 BFD 或 NQA。

```
<H3C>display current-configuration | include 192.168.2.0
ip route-static192.168.2.0 255.255.255.0 GigabitEthernet0/0 192.168.1.2 bfd control-packet

<H3C>display current-configuration | include 192.168.2.0
ip route-static192.168.2.0 255.255.255.0 192.168.1.2 track 1
```

（5）检查 BFD 或 NQA 配置与状态

在配置了静态路由与 BFD 或 NQA 联动的情况下，查看相关配置、状态信息是否正确。正常情况下 BFD 的会话状态为 Up；NQA track 项的状态信息为 Positive。

命令：*display bfd session*

或　　*display track xxx*（静态路由绑定的 track 号）

例如：通过上述命令查看，可以确认 BFD 或 NQA 状态正常。

```
<H3C>display bfd session
 Total Session Num: 1              Init Mode: Active
 IPv4 Session Working Under Ctrl Mode:
 LD/RD          SourceAddr      DestAddr       State   Holdtime   Interface
 53/53          192.168.1.1     192.168.2.2    Up      3300ms     GE0/0

<H3C>display track 1
Track ID: 1
Status: Positive(notify 13 seconds later)
Notification delay: Positive 20, Negative 30 (in seconds)
Reference object:
NQA entry: admin test
Reaction: 10
```

（6）检查静态路由的优先级

检查去往同一目的网段的路由中，静态路由的优先级是否最高。

命令：*display ip routing-table xxx.xxx.xxx.xxx*（目的 IP 网段）

　　　display ip routing-table xxx.xxx.xxx.xxx（目的 IP 网段）*verbose*

例如：通过上述命令查看，可以确认静态路由的优先级不是最高，因而未出现在全局路由表中。

```
<H3C>display ip routing-table 192.168.2.0
Routing Tables: Public
            Destinations : 1        Routes : 1
Destination/Mask      Proto    Pre   Cost          NextHop        Interface
192.168.2.0/24        OSPF     10    2             192.168.1.2    GE0/0

[H3C]display ip routing-table 192.168.2.0 verbose
Routing Table : Public
Summary Count :2
   Destination: 192.168.2.0/24
      Protocol: OSPF          Process ID: 1
    Preference: 10                  Cost: 2
       NextHop: 192.168.1.2    Interface: GigabitEthernet0/0
     BkNextHop: 0.0.0.0      BkInterface:
   RelyNextHop: 0.0.0.0        Neighbor : 0.0.0.0
     Tunnel ID: 0x0                Label: NULL
         State: Active Adv           Age: 00h00m23s
           Tag: 0
   Destination: 192.168.2.0/24
      Protocol: Static        Process ID: 0
    Preference: 60                  Cost: 0
       NextHop: 192.168.3.2    Interface: GigabitEthernet0/1
     BkNextHop: 0.0.0.0      BkInterface:
   RelyNextHop: 0.0.0.0        Neighbor : 0.0.0.0
     Tunnel ID: 0x0                Label: NULL
         State: Inactive Adv         Age: 00h21m52s
           Tag: 0
```

(7) 检查静态路由掩码长度

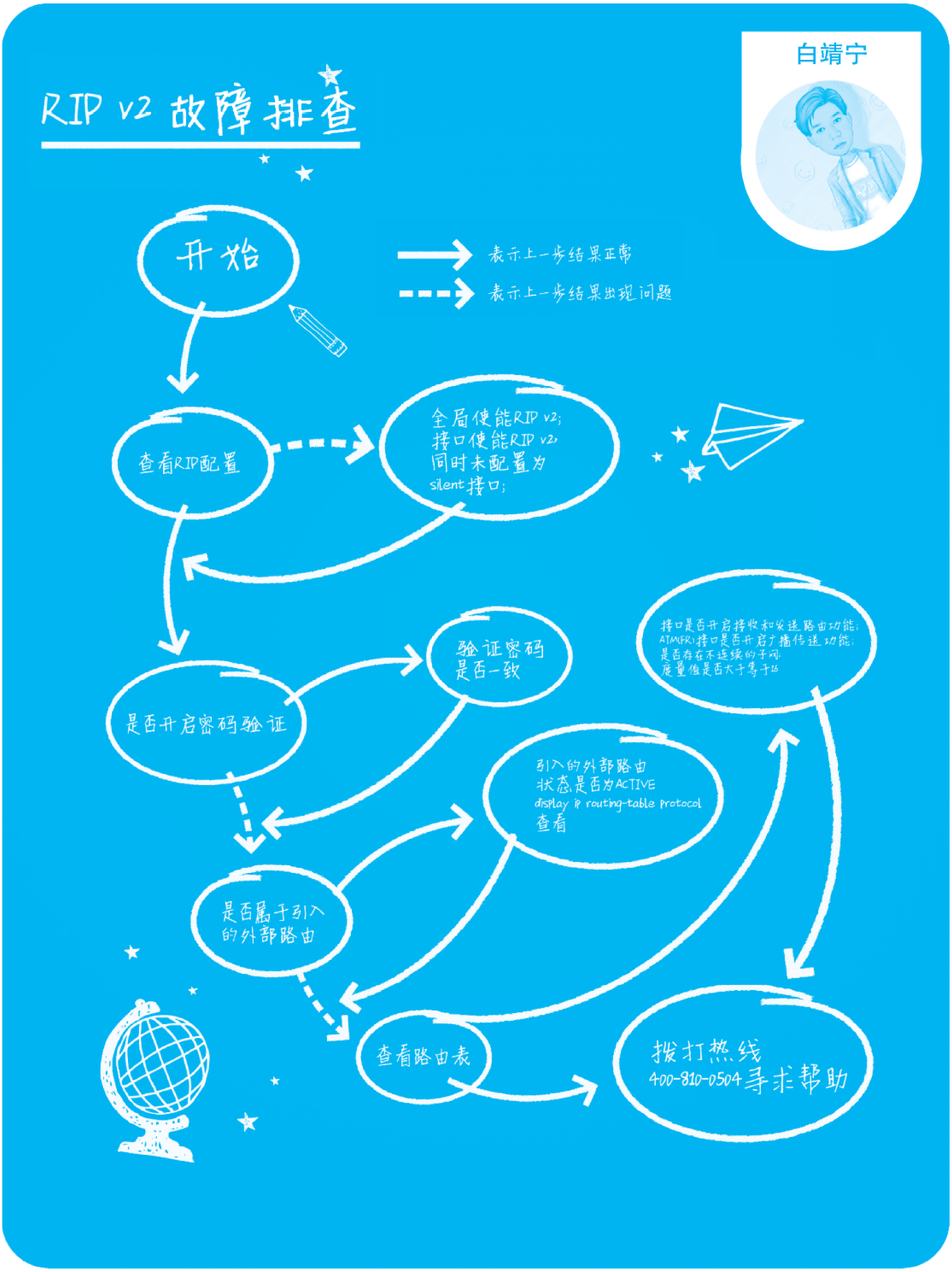
检查到目的 IP 网段的报文转发能否匹配静态路由，即检查该静态路由的掩码是否最长。

命令：*display ip routing-table xxx.xxx.xxx.xxx*(目的 IP 网段)

例如：通过上述命令查看，可以确认静态路由的掩码不是最长。

```
<H3C>display ip routing-table 192.168.2.0
Routing Table : Public
Summary Count : 2

Destination/Mask   Proto   Pre   Cost   NextHop       Interface
192.168.2.0/24     Static  60    0      192.168.1.2   GE0/0
192.168.2.0/25     RIP     100   1      192.168.3.2   GE0/1
```



白靖宁
RIP v2 故障排查
开始
表示上一步结果正常
表示上一步结果出现问题
查看RIP配置
全局使能RIP v2;
接口使能RIP v2;
同时未配置为
silent接口;
是否开启密码验证
验证密码
是否一致
接口是否开启接收和发送路由功能;
ATM(FR)接口是否开启广播传送功能;
是否存在不连续的子网;
度量值是否大于等于16
引入的外部路由
状态是否为ACTIVE
display ip routing-table protocol
查看
是否属于引入
的外部路由
查看路由表
拨打热线
400-810-0504寻求帮助

01 公共协议 > 1.1 IP 路由 > 1.1.2 RIPv2 故障排查 > 步骤详解

1. 开始

RIP 是一种较为简单的内部网关协议，维护起来较为容易，通常情况下只要参数配置正确，就能够计算出正确的路由表。当发生路由表缺失现象时，首先需要检查 RIP 的各种参数设置，是否正确启动，接口功能是否使能。

因此定位思路是，先查基本配置，再查看是否验证问题，是否引入外部路由，路由表是否完整。

2. 流程图相关操作说明

(1) 查看 RIP 配置

查看 RIP 进程的当前运行状态及配置信息。

命令：*display rip*

例如：通过命令查看，确认全局正确使能 RIPv2 并且接口未设置成 silent 端口。

```
<H3C> display rip
  Public VPN-instance name :

    RIP process :1
      RIP version : 2
      Preference : 100
      Checkzero : Enabled
      Default-cost : 0
      Summary : Enabled
      Hostroutes : Enabled
      Silent interfaces : None
      Default routes : Only   Default route cost : 3
      Verify-source : Enabled
      Networks : 192.168.1.0
      Configured peers : None
```

(2) 是否开启密码验证

查看使能 RIP 的端口是否开启密码验证功能，如果开启，确保对端端口同样开启密码验证功能，同时验证密码一致。

命令：接口视图下 *display this*

例如：通过命令查看接口是否开启密码验证。

```
[H3C-GigabitEthernet0/1]display this
 #
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.4.1 255.255.255.0
rip authentication-mode md5 rfc2453 =W6JJ'N_LBKQ=^Q'MAF4<1!!
rip version 2 multicast
 #
```

如果端口下配置了密码，需要确保两端密码配置一致。由于密文配置的密码采用了加密

显示，在无法确定密码是否一致的情况下，请重新配置确认密码一致。

命令：接口视图下 *rip authentication-mode*

例如：在接口 GigabitEthernet0/1 上配置 rfc 2453 格式的 md5 验证，验证字为 rose。

```
<H3C> system-view
[H3C] interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1]rip version 2
[H3C-GigabitEthernet0/1]rip authentication-mode md5 rfc2453 rose
```

（3）是否属于引入的外部路由

在 RIP 在引入外部路由时，只能引入路由表中状态为 Active 的路由，是否为 Active 状态通过命令查看。

命令：*display ip routing-table protocol*

例如：以静态路由为例，通过命令来查看引入的静态路由是否为 Active 状态。

```
[H3C]display ip routing-table protocol static 192.168.2.0
...
Static Routing Table Status : <Active>
Summary Count :1
Destination/Mask      Proto   Pre   Cost         NextHop        Interface
192.168.2.0/24        Static  60    0             192.168.1.2    GE0/0
```

（4）查看路由表

查看 RIP 路由表中是否存在相应路由。

命令：*display rip 1 route xxx.xxx.xxx.xxx*

例如：查看 RIP 路由表中 56.0.0.0/8 网段的路由信息。

```
<H3C> display rip 1 route 56.0.0.0/8
 Route Flags: R-RIP, T-TRIP
P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
--------------------------------------------------------------------------
Peer 21.0.0.23 on Vlan-interface11
Destination/Mask        NextHop     Cost   Tag   Flags     Sec
56.0.0.0/8              21.0.0.23   1      0     RA        102
Peer 21.0.0.12 on Vlan-interface12
Destination/Mask        NextHop     Cost   Tag   Flags     Sec
56.0.0.0/8              21.0.0.12   1      0     RA        34
```

① 接口是否开启接收和发送路由的功能。若查看 RIP 路由表未发现相应路由信息，请确认对应的接口未关闭发送和接收 RIP 报文的功能。

命令：*display rip 1 interface*

```
<H3C> display rip 1 interface
Interface-name: Vlan-interface11
        Address/Mask:1.1.1.1/24           Version:RIPv1
        MetricIn:5        MetricIn route policy:123
        MetricOut:5       MetricOut route policy:234
        Split-horizon/Poison-reverse:on/off          Input/Output:on/on
        Current packets number/Maximum packets   number:234/2000
```

如果通过上述命令查看到 rip Input/Output 存在 off 状态，可以通过命令将其修改为 on 状态，在修改前，请确认该端口是否的确需要将 rip Input/Output 置于 off 状态。

命令：接口视图下 *rip input/output*

```
<H3C>system-view
[H3C]interface GigabitEthernet 0/1
[H3C-GigabitEthernet0/1]rip input
```

② 如果在 ATM 和 FR 接口上配置 RIP，确保开启了接口的广播传送功能。以 ATM 接口为例，在对应的接口开启接收 RIP 报文的情况下，使能了 RIP 的 Atm 链路上无法传送 RIP 路由时，确认在 pvc 上开启了广播功能。

命令：*display current-configruation interface atm*

例如：通过命令查看使能了 RIP 的 Atm 配置信息。

```
<H3C> display current-configruation interface atm
#interface Atm3/1/0
pvc 2 1/32
map ip 10.0.0.1 broadcast
```

如果对应 pvc 没有使能广播功能，请在创建映射时配置使能广播功能。

命令：*map ip xxx.xxx.xxx.xxx*

例如：在 pvc 1/32 上创建一个静态映射，指定对端 IP 地址为 10.0.0.1，并支持广播。

```
<H3C> system-view
[H3C] interface atm 3/1/0
[H3C-Atm3/1/0] pvc 2 1/32
[H3C-atm-pvc-Atm3/1/0-1/\32] map ip 10.0.0.1 broadcast
```

③ 是否存在不连续的子网。如果本地路由表中缺失的路由信息和本地路由表中存在的路由信息属于不连续的子网，则需要取消接口的聚合功能。summary 命令用来使能 RIP-2 自动路由聚合功能，聚合后的路由以使用自然掩码的路由形式发布，减小了路由表的规模。undo summary 命令用来关闭自动路由聚合功能，以便将所有子网路由广播出去。

命令：*undo summary*

例如：本地存在 162.16.1.0/24 网段，无法学习到邻居路由器上的 162.16.3.0/24 网段路由信息。

```
<H3C> system-view
[H3C] rip
[H3C-rip-1] undo summary
```

④ 度量值是否大于等于 16。如果本地路由表无相关路由，请查看存在该路由的相邻路由器上该路由的度量值，并且确认该度量值和该设备端口配置的发送路由度量附加值以及本设备端口配置的接收路由的附加度量值(如果有)之和小于 16。

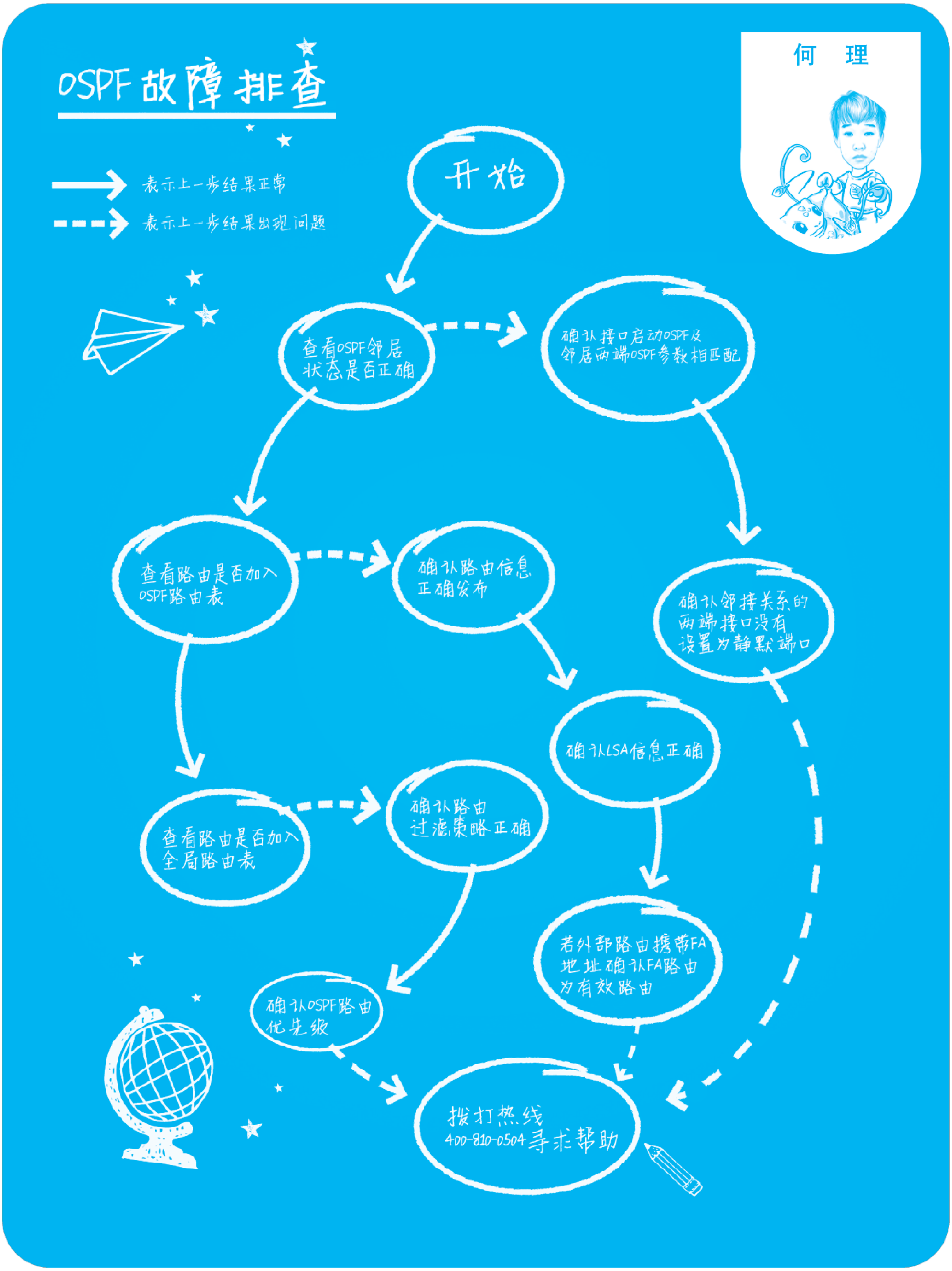
查看路由度量值的命令：*display rip 1 database*

```
[H3C] interface GigabitEthernet 2/1/2
[H3C-GigabitEthernet2/1/2] display rip 1 database
        1.1.1.0/24, cost 2, nexthop 1.1.1.1, Rip-interface
```

查看接口附加度量值的命令：*display rip 1 interface*

```
<H3C> display rip 1 interface
Interface-name: Vlan-interface11
        Address/Mask:1.1.1.1/24        Version:RIPv1
        MetricIn:5        MetricIn route policy:123
        MetricOut:5       MetricOut route policy:234
```

通过上述命令查看接口的 MetricIn 是接收路由的附加度量值，MetricOut 是发送路由的附加度量值。


OSPF故障排查
何 理
表示上一步结果正常
表示上一步结果出现问题
开始
查看OSPF邻居状态是否正确
确认接口启动OSPF及邻居两端OSPF参数相匹配
确认邻接关系的两端接口没有设置为静默端口
查看路由是否加入OSPF路由表
确认路由信息正确发布
确认LSA信息正确
查看路由是否加入全局路由表
确认路由过滤策略正确
若外部路由携带FA地址确认FA路由为有效路由
确认OSPF路由优先级
拨打热线 400-810-0504寻求帮助

01 公共协议 > 1.1 IP 路由 > 1.1.3 OSPF 故障排查 > 步骤详解

1. 开始

由于 OSPF 路由正确地加入到全局路由表，依赖于正确的 OSPF 路由计算，而 OSPF 计算路由依赖于正确的 OSPF LSDB 数据库信息，要建立正确的 OSPF LSDB 数据库则首先要确保邻居之间能够形成正确的邻接关系。因此 OSPF 路由问题的排查整体思路为：首先检查 OSPF 邻居关系，其次检查 OSPF LSDB 数据库信息，最后检查全局路由表。

2. 流程图相关操作说明

(1) 查看 OSPF 邻居状态是否正确

查看两端 OSPF 邻居状态是否正常，正常情况下 DRother 之间的邻居关系应该稳定在 2-way 状态，非 DRother 之间的邻居关系应该稳定在 Full 状态。

命令：*display ospf peer x.x.x.x*

例如：通过命令查看，可以确认 OSPF 的邻居状态是否正常。

```
<H3C>display ospf peer 2.2.2.2

                OSPF Process 1 with Router ID 1.1.1.1
                      Neighbor Brief Information
  Area: 0.0.0.0
Router ID        Address          Pri Dead-Time  Interface        State
2.2.2.2          10.1.1.2         1   35         Eth0/1/0.2       Full/BDR
```

(2) 确认接口启动 OSPF 及邻居两端 OSPF 参数相匹配

① 确认接口启动 OSPF。OSPF 的运行是基于设备接口的，如果 OSPF 没有在接口启动，那么邻居关系肯定无法形成。在接口上启用 OSPF 是通过 Area 视图下的 network 命令实现的，必须确保 network 中的网络范围包括需要启动 OSPF 的接口地址。

命令：*display ospf interface*

例如：通过命令查看接口是否启动 OSPF。

```
<H3C>display ospf interface
            OSPF Process 1 with Router ID 3.3.3.3
                    Interfaces
 Area: 0.0.0.0
 IP Address       Type        State    Cost  Pri   DR           BDR
 12.1.1.1         Broadcast DR         1     1     12.1.1.1     12.1.1.2
```

② 确认邻居两端 OSPF 参数相匹配，具体包括以下几点。

(a) OSPF 区域配置是否匹配。启动 OSPF 的接口属于某个区域，同时区域有多种类型，区域依靠区域 ID 进行标识，如果两边的区域类型或区域 ID 不匹配，则不会形成邻居关系。

(b) OSPF 验证配置是否匹配。OSPF 支持报文验证功能，验证分为简单验证和 md5 验证两种类型，如果两边验证类型或密钥配置不同，则 OSPF 无法通过验证，邻居关系无法形成。

(c) 两端 OSPF 接口上计时器设定值是否匹配。OSPF 通过周期性的交互 Hello 报文维系邻居关系，Hello 报文中携带了 Hello 报文的发送间隔计时器及邻居失效计时器，如果这些

计时器的值在两边的 Hello 报文中不匹配，那么 OSPF 的邻居关系无法形成。注意 dead timer 的值至少应为 hello timer 值的 4 倍。

(d) 两端 OSPF 接口类型是否匹配。OSPF 邻居关系的正常建立需要确保邻居两端接口的 OSPF 网络类型一致，否则将无法形成邻居关系。需要说明的是若邻居双方一端设置为 P2P 类型另一端设置为广播类型，那么邻居状态可以达到 FULL 状态，但此时无法计算出路由信息。

(e) 广播网络中两端接口子网掩码是否相同。OSPF Hello 报文中携带子网掩码信息。在广播网络中，如果两端接口属于不同的 IP 子网，那么邻居关系无法形成。

(f) NBMA 网络是否指定邻居。OSPF 网络类型为 NBMA 时必须手工指定邻居的 IP 地址，否则端口无法发送 Hello 报文，无法形成邻居关系。

命令：*display current-configuration interface interface-number*

display current-configuration configuration interface interface-number

例如：通过命令查看接口下的 OSPF 参数设置是否一致。

```
<H3C>display current-configuration interface e0/1/0.1
#
interface Ethernet0/1/0.1
 vlan-type dot1q vid 100
 ip address 20.1.1.1 255.255.255.0
 ospf network-type p2p
<H3C>display current-configuration interface e0/1/0.1
#
interface Ethernet0/1/0.1
 vlan-type dot1q vid 100
 ip address 20.1.1.2 255.255.255.0
 ospf network-type p2p
```

(3) 确认邻接关系的两端接口没有设置为静默端口

当接口在 OSPF 协议视图中被设置为静默端口时，它将不能发送 OSPF Hello 报文，因此 OSPF 邻居关系无法形成。

命令：*display current-configuration configuration ospf*

例如：通过命令查看接口正确启动 OSPF 并设置为非静默端口，配置静默端口。

```
<H3C>display current-configuration configuration ospf
#
ospf 1
 silent-interface GigabitEthernet 2/0/1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
 area 0.0.0.1
  network 20.1.1.1 0.0.0.0
  network 10.10.2.1 0.0.0.0
```

(4) 查看路由是否加入 OSPF 路由表

查看 OSPF 路由表中是否存在相应路由。

命令：*display ospf routing x.x.x.x*

例如：查看外部路由 9.9.9.9 是否加入 ospf 路由表。

```
<H3C>display ospf routing 9.9.9.9

          OSPF Process 1 with Router ID 4.4.4.4
                   Routing Tables
Routing for ASEs
 DestinationCost    Type    Tag       NextHop       AdvRouter
 9.9.9.9/321        Type2   1         10.10.5.1     3.3.3.3
```

(5) 确认路由信息正确发布

若查看 OSPF 路由表未发现相应路由信息，请首先确认路由信息是否在 OSPF 中正确发布，对于未进行发布的路由请修改配置将路由正确发布。

命令：*display current-configuration configuration ospf*

例如：查看 10.10.4.0 0.0.0.255 的路由信息是否在 OSPF 中发布。

```
<H3C>display current-configuration configuration ospf
#
ospf 1
 area 0.0.0.0s
  network 10.10.1.0 0.0.0.255
network 10.10.4.0 0.0.0.255
  area 0.0.0.1
network 10.10.2.0 0.0.0.255
```

(6) 确认 LSA 信息正确

确认 OSPF LSDB 数据库中是否存在路由计算所需的正确 LSA 信息。对于区域内的路由需要检查是否存在该路由始发者的 Router LSA，DR 的 Network LSA(广播网络)；对于区域间的路由需要首先检查是否存在 LS ID 为该网段的 Summary LSA，然后检查是否存在该 Summary LSA 所对应 Adv Rtr 的 Router LSA；如果外部路由是通过区域内学习到的，需要首先检查是否存在 LS ID 为该网段的 ASE LSA，然后检查是否存在该 ASE LSA 中所对应 Adv Rtr 的 Router LSA；如果外部路由是通过区域间学到的那么首先检查对应的 ASE LSA，其次检查是否存在该 ASE LSA 所对应 Adv Rtr 的 Asbr Sumarry LSA，最后检查该 Asbr Summary LSA 所对应 Adv Rtr 的 Router LSA。

命令：*display ospf lsdb router x.x.x.x*

display ospf lsdb network

display ospf lsdb summary xxx.xxx.xxx.xxx

display ospf lsdb asbr x.x.x.x

display ospf lsdb ase x.x.x.x

例如：通过命令查看外部路由 9.9.9.9 相关的 LSA 信息。

```
<H3C>display ospf lsdb ase 9.9.9.9
          OSPF Process 1 with Router ID 4.4.4.4
                  Link State Database
    Type        : External
    LS ID       : 9.9.9.9
    Adv Rtr     :3.3.3.3
    LS Age      : 841
    Len         : 36
    Options     :  E
```

```
<H3C>display ospf lsdb asbr 3.3.3.3
              OSPF Process 1 with Router ID 4.4.4.4
                           Area: 0.0.0.2
                    Link State Database
    Type          : Sum-Asbr
    LS ID         : 3.3.3.3
    Adv Rtr       :2.2.2.2
    LS Age        : 1091
    Len           : 28
    Options       :   E
<H3C>display ospf lsdb router 2.2.2.2
              OSPF Process 1 with Router ID 4.4.4.4
                           Area: 0.0.0.2
                    Link State Database
    Type          : Router
    LS ID         : 2.2.2.2
    Adv Rtr       : 2.2.2.2
       Link Count: 1
       Link ID  : 10.10.5.1
       Data     :10.10.5.1
       Link Type: TransNet
       Metric   : 1
```

例如：通过命令查看区域内路由 10.10.4.0/24 相关的 LSA 信息。

```
<H3C>display ospf lsdb network

              OSPF Process 1 with Router ID 2.2.2.2
                           Area: 0.0.0.0
                    Link State Database
    Type          : Network
    LS ID         : 10.10.1.1
 Adv Rtr          : 1.1.1.1
    LS Age        : 934
    Len           : 32
    Options       :   E
    Seq#          : 80000002
    Checksum      : 0xc76b
    Net Mask      : 255.255.255.0
       Attached Router      2.2.2.2
       Attached Router      1.1.1.1
<H3C>display ospf lsdb router 1.1.1.1
              OSPF Process 1 with Router ID 2.2.2.2
                           Area: 0.0.0.0
                    Link State Database
    Type          : Router
    LS ID         : 1.1.1.1
    Adv Rtr       : 1.1.1.1
    LS Age        : 265
    Len           : 48
    Options       :   ABR   E
    Seq#          : 80000007
    Checksum      : 0x8d61
    Link Count    : 2
```

```
        Link ID     : 10.10.1.1
        Data        : 10.10.1.1
        Link Type   : TransNet
        Metric      : 1
        Link ID     : 10.10.4.0
        Data        : 255.255.255.0
        Link Type: StubNet
        Metric      : 1
```

例如：通过命令查看区域间路由 10.10.2.0/24 相关的 LSA 信息。

```
<H3C>display ospf lsdb summary 10.10.2.0
            OSPF Process 1 with Router ID 2.2.2.2
                    Area: 0.0.0.0
                Link State Database
    Type        : Sum-Net
    LS ID       : 10.10.2.0
    Adv Rtr     : 1.1.1.1
    LS Age      : 1400
    Len         : 28
    Options     :   E
    Seq#        : 80000001
    Checksum    : 0x46fb
    Net Mask    : 255.255.255.0
    Tos 0    Metric: 1
<H3C>display ospf lsdb router 1.1.1.1
            OSPF Process 1 with Router ID 2.2.2.2
                    Area: 0.0.0.0
                Link State Database
    Type        : Router
    LS ID       : 1.1.1.1
    Adv Rtr     : 1.1.1.1
    LS Age      : 823
    Len         : 48
    Options     :   ABR   E
    Seq#        : 80000007
    Checksum    : 0x8d61
    Link Count  : 2
        Link ID : 10.10.1.1
        Data    : 10.10.1.1
        Link Type: TransNet
        Metric  : 1
        Link ID : 10.10.4.0
        Data    : 255.255.255.0
        Link Type: StubNet
        Metric  : 1
```

导致 OSPF 数据库中 LSA 异常或缺失的原因主要包括如下几种情况，需要从相关的配置或规划角度进行修正。

① 骨干区域被分割，导致 LSA 缺失。

② 虚连接配置错误，导致 LSA 缺失。

③ RouterID 冲突，导致 LSA 震荡。

(7) 若外部路由携带 FA 地址确认 FA 路由为有效路由

若外部路由携带 FA 地址确认 FA 路由为有效路由。OSPF 必须能够通过区域内或区域

间路由到达该 FA 地址，否则该外部路由不会加入 OSPF 路由表。

例如：外部路由 9.9.9.9 携带了 FA 地址为 10.10.6.2，通过 OSPF 内部路由能够学习到 10.10.6.2 的路由，外部路由 9.9.9.9 正确加入路由表。

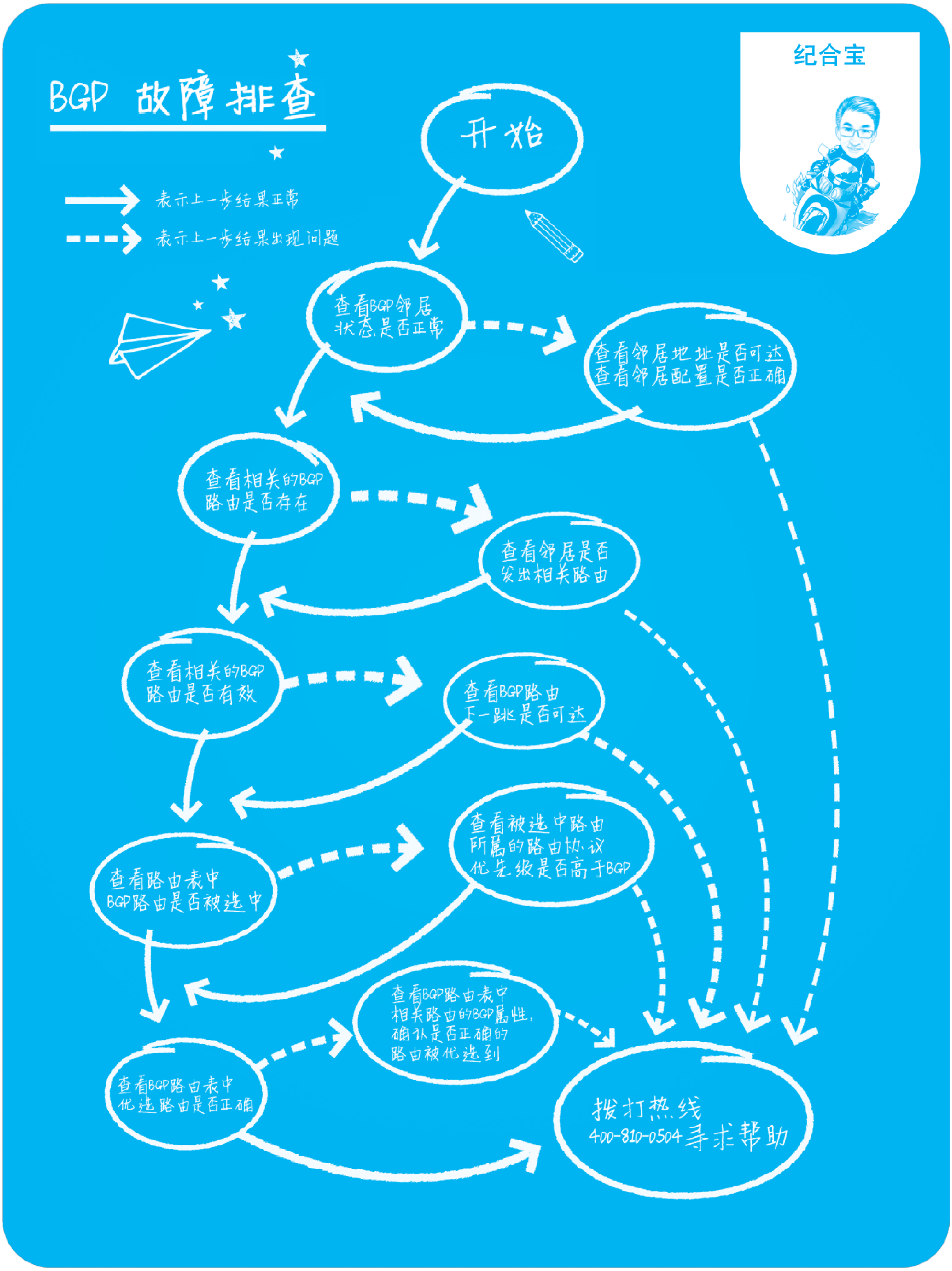
```
<H3C>display ospf lsdb ase 9.9.9.9
          OSPF Process 1 with Router ID 4.4.4.4
                  Link State Database
    Type         : External
    LS ID        : 9.9.9.9
    Adv Rtr      : 3.3.3.3
    LS Age       : 841
    Len          : 36
    Options      :   E
    Seq#         : 80000005
    Checksum     : 0x4e32
    Net Mask     : 255.255.255.255
    TOS 0    Metric: 1
    E Type       : 2
    Forwarding Address :10.10.6.2
    Tag          : 1
<H3C>display ospf routing
         OSPF Process 1 with Router ID 4.4.4.4
                 Routing Tables
 Routing for Network
 Destination      Cost  Type   NextHop     AdvRouter   Area
 10.10.6.0/24     3     Inter  10.10.5.1   2.2.2.2     0.0.0.0
```

（8）查看路由是否加入全局路由表

查看 OSPF 路由是否正确加入到全局路由表内，只有加入到全局路由表的路由才能指导数据包的转发。如果相同的路由信息同时也从其他路由协议学到，为了确保 OSPF 学习的路由能够最终加入全局路由表，需要确保其优先级为最优。

命令：*display ip routing-table x.x.x.x verbose*

```
<H3C>display ip routing-table 9.9.9.9 verbose
Routing Table : Public
Summary Count : 2
    Destination: 9.9.9.9/32
       Protocol: O_ASE          Process ID: 1
     Preference: 150                  Cost: 1
        NextHop: 10.10.1.1       Interface: Ethernet0/1/0
      BkNextHop: 0.0.0.0       BkInterface:
    RelyNextHop: 0.0.0.0        Neighbor : 0.0.0.0
      Tunnel ID: 0x0                 Label: NULL
          State: Active Adv            Age: 00h52m12s
            Tag: 1
    Destination: 9.9.9.9/32
       Protocol: Static         Process ID: 0
     Preference: 200                  Cost: 0
        NextHop: 0.0.0.0         Interface: NULL0
      BkNextHop: 0.0.0.0       BkInterface:
    RelyNextHop: 0.0.0.0        Neighbor : 0.0.0.0
      Tunnel ID: 0x0                 Label: NULL
          State: Inactive Adv          Age: 00h00m26s
            Tag: 0
```



纪合宝
BGP 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看BGP邻居状态是否正常
查看邻居地址是否可达
查看邻居配置是否正确
查看相关的BGP路由是否存在
查看邻居是否发出相关路由
查看相关的BGP路由是否有效
查看BGP路由下一跳是否可达
查看路由表中BGP路由是否被选中
查看被选中路由所属的路由协议优先级是否高于BGP
查看BGP路由表中优选路由是否正确
查看BGP路由表中相关路由的BGP属性，确认是否正确的路由被优选到
拨打热线
400-810-0504寻求帮助

1. 开始

为了保证 BGP 路由正确加入到全局路由表中，首先需要确保 BGP 路由有效，其次要确保能够在和通过其他路由协议学到的路由比较中被优选。

BGP 故障定位思路：首先，查看 BGP 邻居状态；其次，查看 BGP 路由表，查看路由是否存在，是否有效，是否优选；最后，查看 BGP 的属性，查看是否优选到了正确的路由。

2. 流程图相关操作说明

(1) 查看 BGP 邻居状态

如果在 BGP 路由表中，未能查到相匹配路由信息，需要查看 BGP 邻居状态是否正常。

命令：*display bgp peer*

例如：通过命令查看 BGP 邻居是否正常。

```
<H3C> display bgp peer
 BGP local router ID :3.3.3.3
 Local AS number : 65009
 Total number of peers :1      Peers in established state : 1
 Peer      AS     MsgRcvd   MsgSent   OutQ   PrefRcv   Up/Down    State
 3.3.3.3   65002    12        10       0       3       00:09:16   Established
```

(2) 查看路由表，确认 BGP 邻居是否可达，查看邻居配置是否正确

如果 BGP 邻居不能正常建立，需要查看路由表确认 BGP 邻居是否可达。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看 BGP 邻居的 IP 地址是否存在匹配的路由。

```
<H3C> display ip routing-table 3.3.3.3
Routing Tables: Public
Destinations :1            Routes : 1
Destination/Mask   Proto   Pre   Cost    NextHop      Interface
  3.3.3.3/32       OSPF    10    1       9.1.1.1      S2/2/0
```

如果 BGP 邻居不能正常建立，还需要查看 BGP 邻居配置是否正确。

命令：*display current-configuration bgp*

例如：通过命令查看 BGP 邻居的配置。

```
<H3C> display current-configuration bgp
bgp 65001
 undo synchronization
 peer3.3.3.3  as-number  65002
```

还需要用同样的方法确认对端设备的配置是否正确。

(3) 查看 BGP 路由表信息，相关路由是否存在

查看 BGP 路由表信息，确认相关路由是否存在于 BGP 路由表中。

命令：*display bgp routing-table x.x.x.x*

例如：通过命令查看，可以确认 BGP 路由表中是否存在相关路由。

```
<H3C> display bgp routing-table 8.1.1.0/24
 Total Number of Routes: 1
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, ^- VPNv4 best, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S- Stale,
               Origin : i - IGP, e - EGP, ? - incomplete
   Network      NextHop     MED     LocPrf    PrefVal    Path/Ogn
 * >i 8.1.1.0/24  9.1.1.1     0       100       0          65002i
```

（4）确认 BGP 邻居是否将路由发送出来

如果 BGP 路由表中未有相关路由，需要确认 BGP 邻居是否将相关路由发送出来。

命令：*display bgp routing-table peer x.x.x.x advertised-routes*

例如：在对端路由器上通过命令查看邻居发送的路由信息。

```
<H3C> display bgp routing-table peer 2.2.2.2 advertised-routes
 Total Number of Routes: 2
 BGP Local router ID is 3.3.3.3
 Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin:i-IGP, e - EGP, ? - incomplete
 Network          NextHop   MED   LocPrf   PrefVal Path/Ogn
 * >8.1.1.0/24    0.0.0.0   0     0                 i
```

（5）查看 BGP 路由表信息，相关路由是否有效

查看 BGP 路由表信息，确认相关路由在于 BGP 路由表中是否有效。

命令：*display bgp routing-table x.x.x.x*

例如：通过命令查看，可以确认 BGP 路由表中相关路由是否有效。

```
<H3C> display bgp routing-table 8.1.1.0 24
 Total Number of Routes: 1
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, ^- VPNv4 best, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale,
               Origin : i - IGP, e - EGP, ? - incomplete
 Network          NextHop     MED      LocPrf    PrefVal    Path/Ogn
 * i 8.1.1.0/24   9.1.1.1     0        100       0          65002i
```

（6）查看路由表，确认 BGP 路由下一跳是否可达

如果 BGP 路由表中存在相应的路由信息，但是该路由为无效路由，需要确认该 BGP 路由下一跳是否可达。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看 BGP 路由的下一跳是否存在匹配的路由。

```
<H3C> display ip routing-table 9.1.1.1
Routing Tables: Public
        Destinations :1          Routes : 1
Destination/Mask   Proto   Pre   Cost    NextHop       Interface
  9.1.1.0/30       OSPF    10    1       127.0.0.1     S2/2/0
```

（7）查看路由表，确认 BGP 路由是否被选中

查看路由表，确认路由表是否优选了 BGP 的路由。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看相关路由是否由 BGP 学习到。

```
<H3C> display ip routing-table 8.1.1.0/24
Routing Tables: Public
        Destinations :1          Routes : 1
Destination/Mask  Proto  Pre  Cost   NextHop     Interface
  8.1.1.0/24      OSPF   10   1      9.1.1.1     S2/2/0
```

(8) 查看路由配置信息，确认路由表中选中路由所属路由协议的优先级是否高于 BGP

查看设备配置信息，确认在路由表中选中的路由所属的路由协议的优先级。

命令：*display current-configuration bgp*

命令：*display current-configuration ospf*

例如：查看 OSPF 路由的优先级是多少，BGP 的路由优先级是多少？注意 H3C 设备默认的各个路由协议优先级。

```
<H3C>display current-configuration

bgp 65001
 router-id2.2.2.2
 preference 170 170 170
 network 10.0.127.0 255.255.255.0

ospf 10 router-id2.2.2.2
 preference ase 190
 area 0.0.0.0
  network 10.0.251.156 0.0.0.3
```

(9) 查看 BGP 路由表，查看 BGP 属性，确认 BGP 是否优选到正确的路由

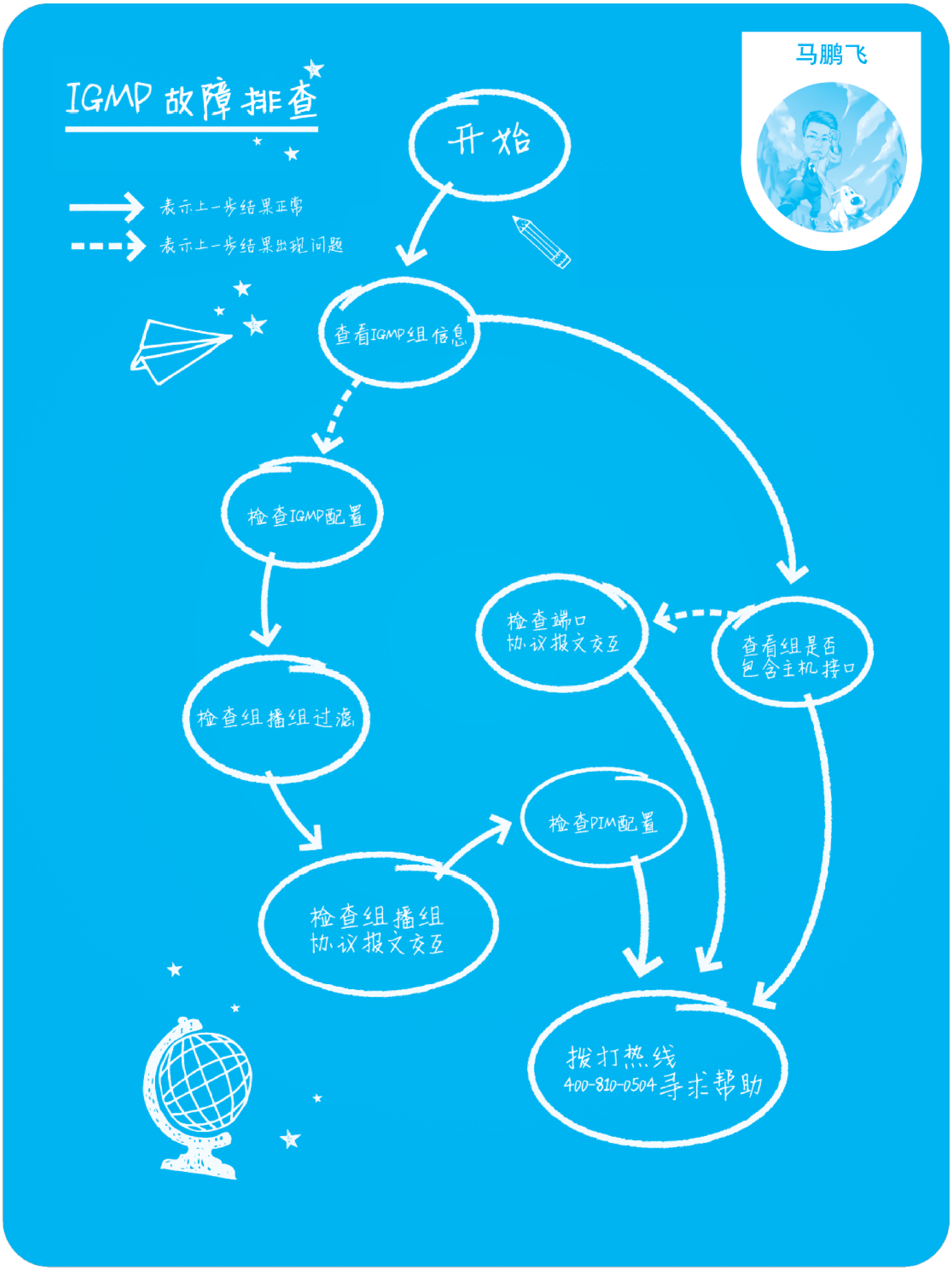
查看 BGP 路由表，确认 BGP 是否优选到正确的路由。

命令：*display bgp routing-table x.x.x.x*

例如：通过命令查看相关 BGP 路由的属性。

```
<H3C> display bgp routing-table 8.1.1.0/24
 Total Number of Routes: 1
 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, ^- VPNv4 best, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale,
               Origin : i - IGP, e - EGP, ? - incomplete
  Network        NextHop     MED      LocPrf    PrefVal  Path/Ogn
* >i 8.1.1.0/24   9.1.1.1     0        100       0        65002i
 * i 8.1.1.0/24  10.1.1.1     0        0         0        65003i
```

常用 BGP 属性比较顺序：①比较 Locprf 属性大小；②比较 AS-Path 的长短；③比较 Origin 属性，i 优先于?；④比较 MED 属性大小；⑤优先选择从 EBGP 邻居学来的路由。


IGMP故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看IGMP组信息
检查IGMP配置
检查组播组过滤
检查组播组
协议报文交互
检查PIM配置
检查端口
协议报文交互
查看组是否
包含主机接口
拨打热线
400-810-0504寻求帮助
马鹏飞

1. 开始

组播分为二层和三层组播协议，其中，IGMP Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组，IGMP 负责 IP 组播成员管理，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系，PIM-DM 和 PIM-SM 是运行在路由器之间或三层交换机之间的三层组播路由协议，通过单播路由协议产生相应的组播路由表项。

IGMP 协议定位故障的思路是：先查组信息，再查配置，最后查报文。

2. 查看 IGMP 组信息

查看设备的 IGMP 组信息，可以检查对应接口或 VLAN 是否作为成员端口加入相应组播组。

例如：通过命令查看，可以确认 Vlan-interface101 下有 IP 为 10.1.1.2 的 Host 加入组播组 225.0.0.1。

命令：***display igmp group*** *group-address*

```
[H3C]display igmp group 225.0.0.1
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 Vlan-interface101(2.1.1.1):
  Total 1 IGMP Group reported
    Group Address    Last Reporter    Uptime      Expires
    225.0.0.1        10.1.1.2         00:15:11    00:01:57
```

3. 查看组是否包含主机接口

查看 IGMP 跟踪的主机信息，检查组播组是否包含正确的主机接口，需要在全局或接口视图下使能主机跟踪功能。

命令：***display igmp host interface*** *interface-type interface-number* ***group*** *group-address*

例如：通过命令查看，可以确认正在接收组播数据的成员主机信息(包括主机的 IP 地址、运行时间和超时时间等)，检查主机是否在 GigabitEthernet2/0/18 下。

```
[H3C] display igmp host interface GigabitEthernet2/0/18 group 225.0.0.1
Host information of VPN-Instance: public net
 GigabitEthernet2/0/18(10.1.1.1):
     (0.0.0.0, 225.0.0.1)
      Host                                    Uptime        Expires
      10.1.1.3                                00:00:14      00:01:56
```

如果想要在设备上查看主机信息，需要在全局或接口下使能主机跟踪功能。

例如：

```
[H3C-igmp]display this
#
```

```
igmp
 host-tracking
#

 [H3C-GigabitEthernet2/0/18]display this
#
interface GigabitEthernet2/0/11
 igmp host-tracking
#
```

4. 检查端口协议报文交互

通过在主机侧抓包,查看当前主机的成员报告报文是否正常发送,设备是否正确回应,协议交互是否正常。

例如:通过设备上 debug IGMP 的 leave 和 report 报文,可以看到设备正常收到主机发来的加入/离开报文。

```
<H3C>debugging igmp leave
<H3C>debugging igmp report
<H3C>terminal monitor
Info: Current terminal monitor is on.
<H3C>terminal debugging
Info: Current terminal debugging is on.

<H3C> * Jan  1 01:46:04:806 2011 H3C IGMP/7/REPORT: Received IGMPv2 report for group 225.1.1.1 on interface Vlan-interface10(1.1.1.1) (G16995)
 * Jan  1 01:46:04:806 2011 H3C IGMP/7/REPORT: Process IS_EX packet for include group(225.1.1.1) on interface Vlan-interface10(1.1.1.1) (G115449)
...

<H3C> * Jan  1 01:57:07:615 2011 H3C IGMP/7/LEAVE: Received IGMPv2 leave for group 225.1.1.1 on interface Vlan-interface10(1.1.1.1) (G16995)
 * Jan  1 01:57:07:616 2011 H3C IGMP/7/REPORT: Process TO_IN packet for exclude group(225.1.1.1) on interface Vlan-interface10(1.1.1.1) (G115449)
...
```

在主机侧抓包,能抓到对应的主机发出的加入/离开报文,如图 1-1 和图 1-2 所示。

IP 为 1.1.1.2 的主机发出加入报文,组播组地址为 225.1.1.1。

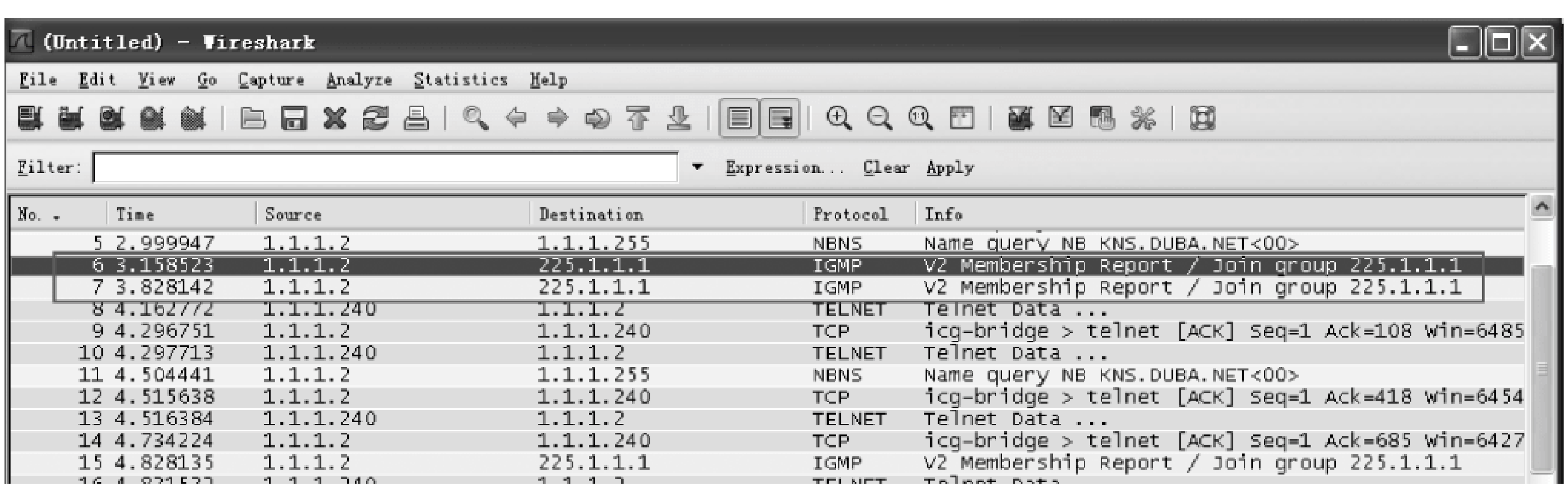


图 1-1 对应主机发出加入报文

主机离开时，向本网段所有路由器发出 Leave Group 报文，目的地址为 224.0.0.2。

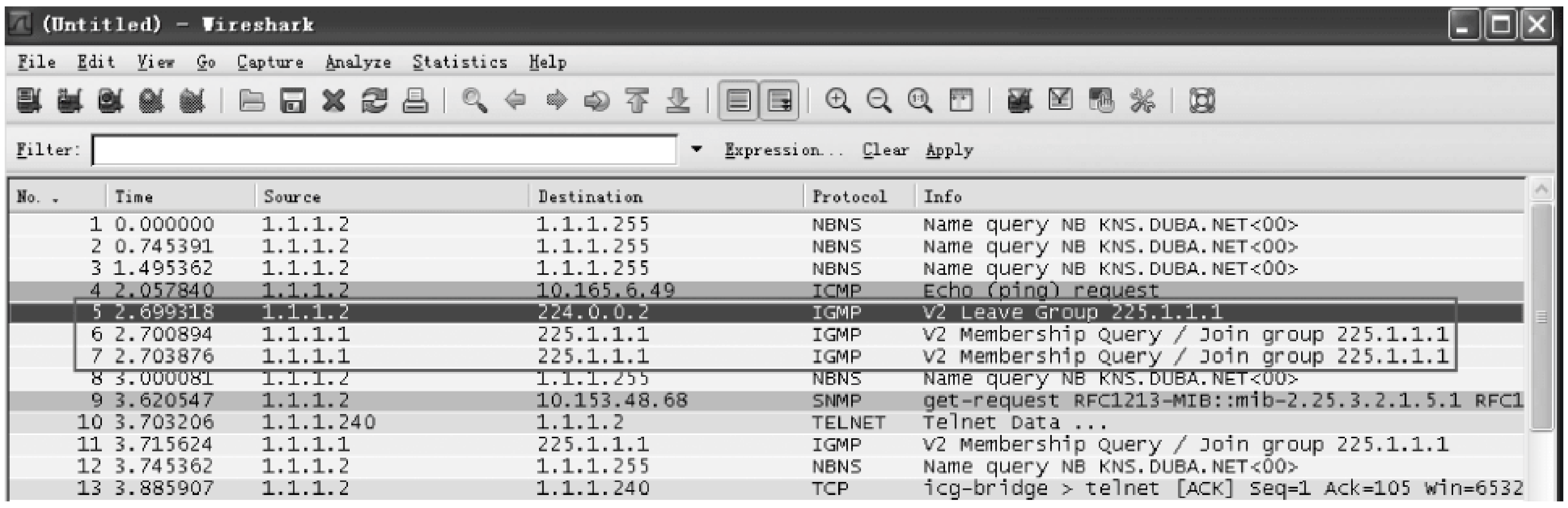


图 1-2 对应主机发出离开报文

5. 检查 IGMP 配置

查看路由器上 IGMP 的版本和参数配置，连接在同一网段的所有路由器最好运行相同版本的 IGMP，且参数配置需要一致，否则将导致 IGMP 组成员关系的混乱。

命令：*display igmp interface verbose*

例如：通过命令查看，可以确认当前路由器的 IGMP 版本为 v2，发送 IGMP 普遍组查询报文的时间间隔为 60 秒，IGMP 其他查询器的存在时间为 125 秒，IGMP 普遍组查询的最大响应时间为 10 秒。

```
[H3C]display igmp interface verbose
Interface information of VPN-Instance: public net
 Vlan-interface101(2.1.1.1):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Value of last member query interval(in seconds): 1
   Value of startup query interval(in seconds): 15
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:20
   Querier for IGMP: 2.1.1.1 (this router)
   IGMP activity: 2 joins, 1 leaves
   Multicast routing on this interface: enabled
   Robustness: 2
   Require-router-alert: disabled
   Fast-leave: disabled
   Ssm-mapping: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
   Proxying interface: None
  Total 1 IGMP Group reported
```

6. 检查组播组过滤

确认是否应用了组播组过滤功能，使能该功能的接口将按照 ACL 规则对收到的 IGMP 成员关系报告报文进行过滤，只为该规则所允许的组播组维护组成员关系。

例如：通过命令查看，接口下的过滤器配置，有匹配 ACL 规则号 3000 的过滤器。

```
[H3C-Vlan-interface101]display this
#
```

```
interface Vlan-interface101
 ip address 2.1.1.1 255.255.255.0
 igmp enable
 igmp group-policy 3000
 pim dm
#
return
```

查看所配置的 ACL 规则，检查是否将所要实现的组播组进行了过滤。

命令：***display acl*** *acl-number*

例如：只需要过滤 IP 地址为 225.0.0.10 的组播组。

```
[H3C]display acl3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 deny ip destination 225.0.0.1 0
 rule 5 permit ip
```

7. 检查组播组协议报文交互

通过在主机侧抓包，查看当前组播组的查询报文是否正常发送，主机是否回应，协议交互是否正常。

例如：通过设备上 debug IGMP 的 Query 报文，可以看到设备正常发出通用查询报文。

```
<H3C>debugging igmp query
<H3C>terminal monitor
Info: Current terminal monitor is on.
<H3C>terminal debugging
Info: Current terminal debugging is on.

<H3C> * Jan  1 02:01:24:599 2011 H3C IGMP/7/QUERY SEND: Send IGMP version 2 general
query on Vlan-interface10(1.1.1.1) to destination 224.0.0.1 (G14299)
 * Jan  1 02:01:30:236 2011 H3C IGMP/7/REPORT: Received IGMPv2 report for group 225.1.1.1
on interface Vlan-interface10(1.1.1.1) (G16995)
```

在主机上抓包，也能看到对应报文，如图 1-3 所示。

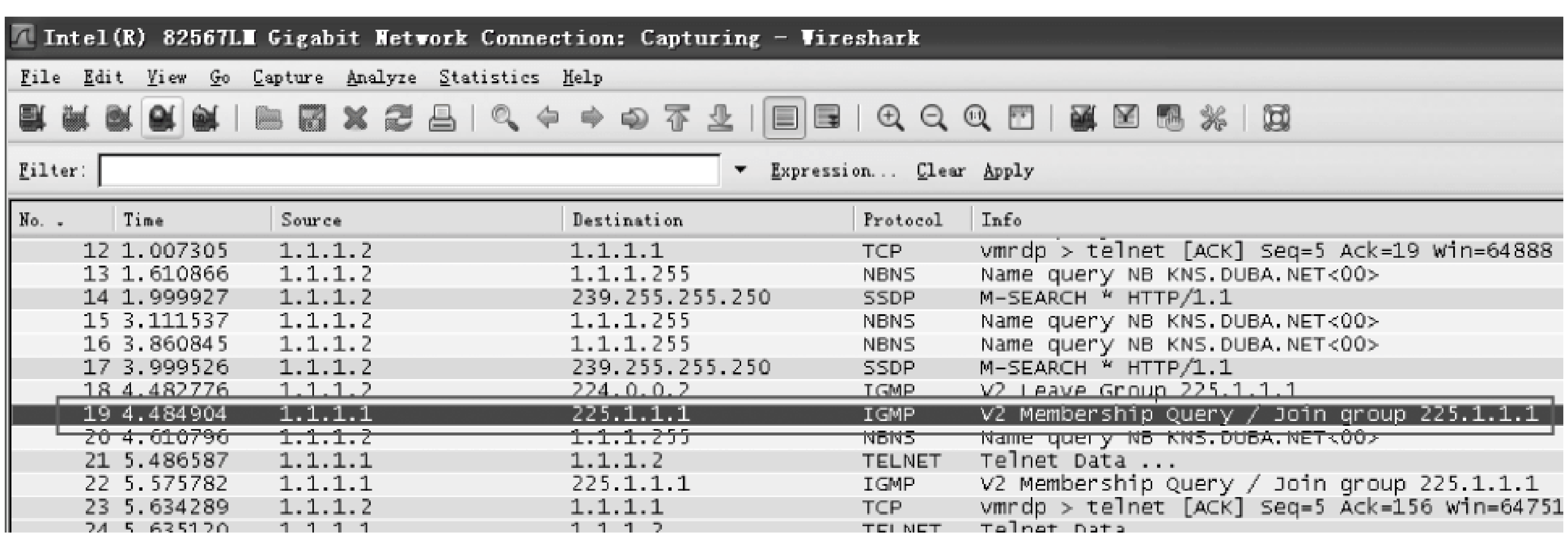
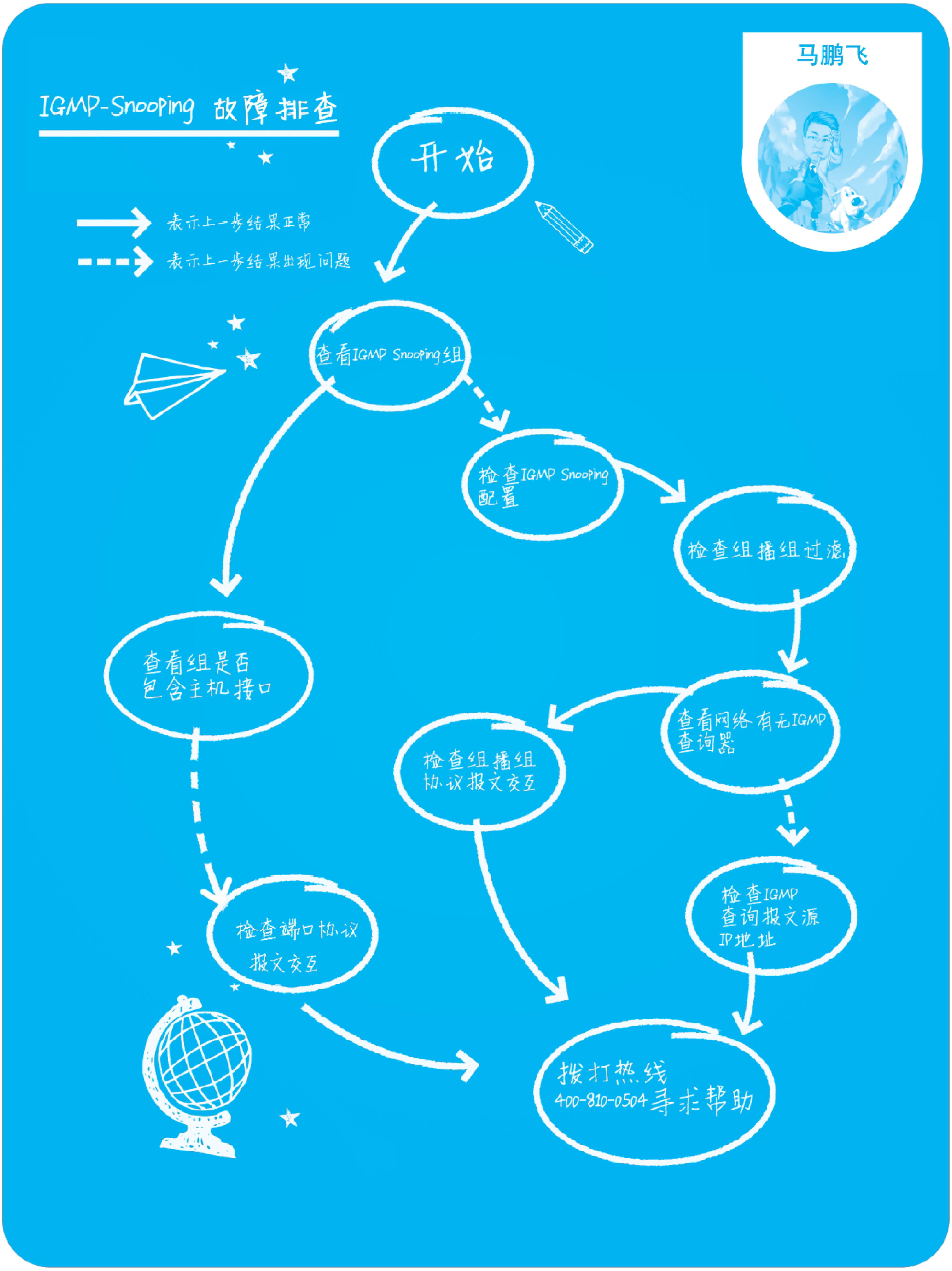


图 1-3　主机抓包对应报文

8. 检查 PIM 配置

如果发现 IGMP 组正常，主机加入正常，但组播流无法收到的情况，查看是否有 PIM 路由，检查 PIM 相关配置。


马鹏飞
IGMP-Snooping 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看IGMP Snooping组
检查IGMP Snooping配置
检查组播组过滤
查看组是否包含主机接口
查看网络有无IGMP查询器
检查组播组协议报文交互
检查端口协议报文交互
检查IGMP查询报文源IP地址
拨打热线 400-810-0504寻求帮助

1. 开始

组播分为二层和三层组播协议，其中，IGMP-Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组，IGMP 负责 IP 组播成员管理，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系，PIM-DM 和 PIM-SM 是运行在路由器之间或三层交换机之间的三层组播路由协议，通过单播路由协议产生相应的组播路由表项。

IGMP-Snooping 协议定位故障的思路是：先查组信息，再查配置，最后查报文。

2. 查看 IGMP-Snooping 组

查看设备的 IGMP-Snooping 组信息，可以检查对应接口或 VLAN 是否作为成员端口加入相应组播组。

例如：通过命令查看，可以确认 GE6/0/1 端口下有 Host 加入组播组 225.0.0.1，VLAN 为 100。

命令：***display igmp-snooping group vlan*** *vlan-id* ***verbose***

```
[H3C]display igmp-snooping group vlan 100 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port unit board: Mask(0x40)
    Router port(s):total 1 port(s).
            GE6/0/2                     (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:225.0.0.1
        (0.0.0.0, 225.0.0.1):
          Attribute:     Host Board
          Host port unit board: Mask(0x40)
          Host port(s):total 1 port(s).
            GE6/0/1                     (D)
    MAC group(s):
      MAC group address:0100-5e00-0001
          Host port unit board: Mask(0x40)
          Host port(s):total 1 port(s).
            GE6/0/1
```

3. 查看组是否包含主机接口

查看 IGMP-Snooping 跟踪的主机信息，检查组播组是否包含正确的主机接口，需要在全局或 VLAN 内使能主机跟踪功能。

命令：***display igmp-snooping host vlan*** *vlan-id* ***group*** *group-address*

例如：通过命令查看，可以确认正在接收组播数据的成员主机信息，检查主机是否在GE6/0/1下。

```
[H3C]display igmp-snooping host vlan 100 group 225.0.0.1
VLAN(ID) : 100
  (0.0.0.0, 225.0.0.1)
    Port : GE6/0/1
      Host                                    Uptime          Expires
      10.1.1.2                                00:12:54        00:03:56
```

如果想要在设备上查看主机信息，需要在全局或VLAN内使能主机跟踪功能。

例如：

```
[H3C-igmp-snooping]display this
#
igmp-snooping
 host-tracking
#

[H3C-vlan10]display this
#
vlan 10
 igmp-snooping enable
 igmp-snooping host-tracking
#
```

4. 检查端口协议报文交互

通过在主机侧抓包，查看当前主机的成员报告报文是否正常发送，设备是否正确回应，协议交互是否正常。

例如：通过设备上debug IGMP-Snooping报文，可以看到设备收到主机发来的加入/离开报文。

```
<H3C>debugging igmp-snooping packet
<H3C>terminal monitor
The current terminal is enabled to display logs.
<H3C>terminal debugging
The current terminal is enabled to display debugging logs.
<H3C>
<H3C>*Jan  1 01:18:53:124 2011 H3C MCS/7/PACKET: Receive IGMPv2 report packet from
port XGE1/0/2 on VLAN 10.
*Jan  1 01:18:53:125 2011 H3C MCS/7/PACKET: The IGMP packet which receive from port
XGE1/0/2 on VLAN 10 on Main slot, forward it locally.
...

<H3C>
*Jan  1 01:23:01:672 2011 H3C MCS/7/PACKET: Receive IGMP leave packet from port XGE1/0/
2 on VLAN 10.
...
```

在主机侧抓包，能抓到对应的主机发出的加入/离开报文，如图 1-4 和图 1-5 所示。

IP 为 1.1.1.2 的主机发出加入报文，组播组地址为 225.1.1.1。

主机离开时，向本网段所有路由器发出 Leave Group 报文，目的地址为 224.0.0.2。

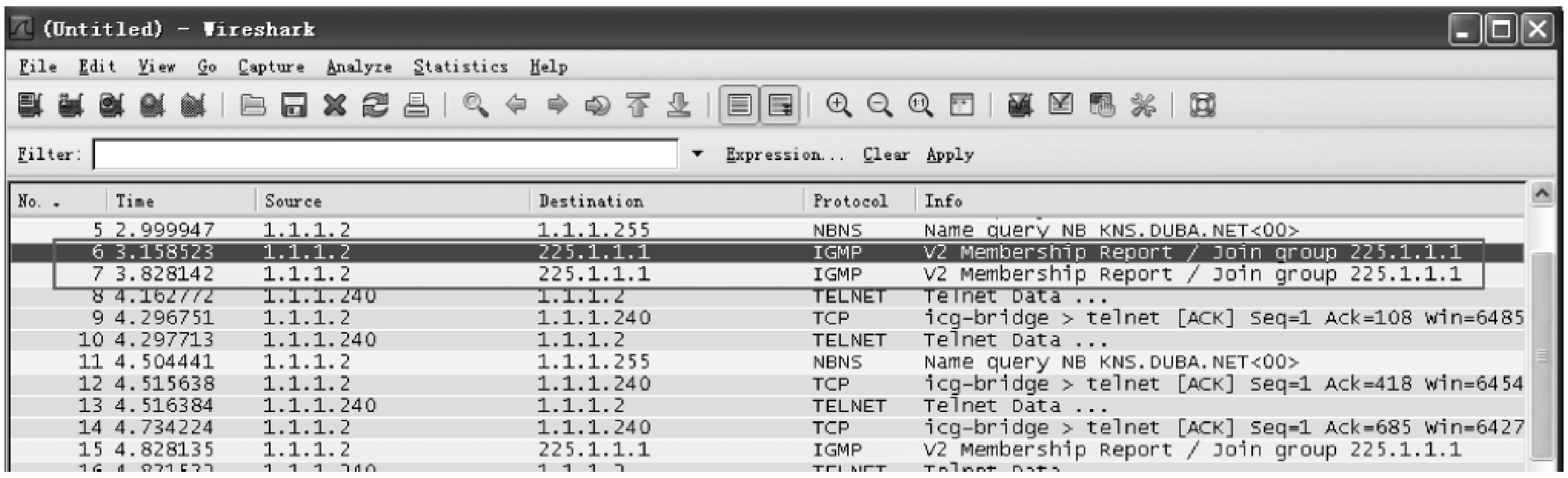


图 1-4 对应主机发出加入报文

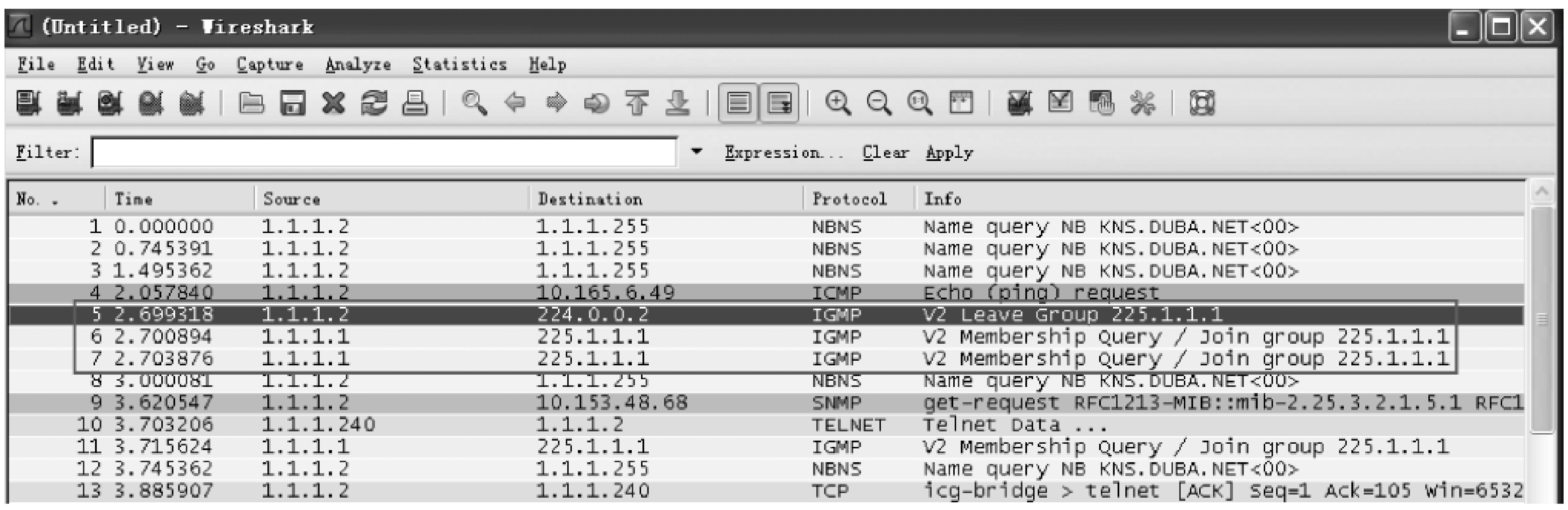


图 1-5 对应主机发出离开报文

5. 检查 IGMP-Snooping 配置

检查设备是否在全局使能了 IGMP-Snooping，以及在相应的 VLAN 中使能了 IGMP-Snooping。检查当前 IGMP-Snooping 版本的配置，是否能够处理主机侧的 Report 报文。

例如：默认情况下，IGMP-Snooping 的版本为 2，能够对 IGMPv1 和 IGMPv2 的报文进行处理，对 IGMPv3 的报文则不进行处理，而是在 VLAN 内将其广播。

命令：***igmp-snooping enable***

igmp-snooping version *version-number*

```
[H3C-vlan100]display this
#
vlan 1
#
vlan 100
 igmp-snooping enable
 igmp-snooping version 3
#
return
```

6. 检查组播组过滤

检查是否正确应用了组播组策略，在全局或接口视图下查看配置。

命令：***igmp-snooping group-policy*** *acl-number* [***vlan*** *vlan-list*]

例如：通过命令查看，配置的组播组策略是否正确。

```
[H3C-igmp-snooping]display this
#
igmp-snooping
 group-policy 3000 vlan 100
#
return

[H3C-GigabitEthernet6/0/1]display this
#
 interface GigabitEthernet6/0/1
  port link-mode bridge
  port access vlan 100
  igmp-snooping group-policy 3000 vlan 100
#
```

查看所配置的 ACL 规则，检查其是否与所要实现的组播组过滤策略相符合。

命令：***display acl*** *acl-number*

例如：只需要过滤 IP 地址为 225.0.0.1 的组播组。

```
[H3C]display acl 3000
Advanced ACL  3000, named -none-, 2 rules,
ACL's

step is 5
 rule 0 deny ip destination 225.0.0.1 0
 rule 5 permit ip
```

7. 查看网络有无 IGMP 查询器

在一个没有三层组播设备的网络中，需要在二层设备上使能 IGMP-Snooping 查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据。查看全网设备中，是否有一台配置了 IGMP 的三层组播路由器充当 IGMP 查询器，或者在二层设备上有查询器配置。

命令：*display current-configuration interface Vlan-interface*

例如：在连接二层设备的接口下配置了 IGMP。

```
[H3C] display current-configuration interface Vlan-interface
#
interface Vlan-interface101
 ip address 2.1.1.1 255.255.255.0
 igmp enable
#
```

例如：在二层设备上配置了查询器。

```
[H3C-vlan10]display this
#
vlan 10
 igmp-snooping enable
```

```
igmp-snooping querier
 igmp-snooping general-query source-ip 1.1.1.1
 igmp-snooping special-query source-ip 1.1.1.1
#
return
```

8. 检查 IGMP 查询报文源 IP 地址

对于收到源 IP 地址为 0.0.0.0 的查询报文的端口，设备不会将其设置为动态路由器端口，从而影响数据链路层组播转发表项的建立，最终导致组播数据无法正常转发，当由二层设备充当 IGMP-Snooping 查询器时，可以把 IGMP 查询报文的源 IP 地址配置为一个有效的 IP 地址以避免上述问题的出现。

命令：*igmp-snooping general-query source-ip* { *ip-address* | ***current-interface*** }

igmp-snooping special-query source-ip { *ip-address* | ***current-interface*** }

例如：通过命令查看，可以确认 VLAN 内配置了 IGMP 普遍组和特定组查询报文源 IP 地址。

```
[H3C-vlan10]display this
#
vlan 1
#
vlan 10
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping querier
 igmp-snooping general-query source-ip 1.1.1.1
 igmp-snooping special-query source-ip 1.1.1.1
#
return
```

9. 检查组播组协议报文交互

通过在主机侧抓包，查看当前组播组的查询报文是否正常发送，主机是否回应，协议交互是否正常。

例如：通过设备上 debug IGMP-Snooping 报文，可以看到设备正常发出通用查询报文。

```
<H3C>
*Jan  1 01:36:06:554 2011 H3C MCS/7/PACKET: Receive IGMPv2 general query packet from port XGE1/0/1 on VLAN 10.
*Jan  1 01:36:06:554 2011 H3C MCS/7/PACKET: The IGMP packet which receive from port XGE1/0/1 on VLAN 10 on Main slot, forward it locally.
*Jan  1 01:36:06:554 2011 H3C MCS/7/PACKET: Broadcast general query packet which receive from port XGE1/0/1 on VLAN 10.
*Jan  1 01:36:06:554 2011 H3C MCS/7/PACKET: Succeed in broadcasting the packet on VLAN 10.
...
```

在主机上抓包，也能看到如图 1-6 对应报文。

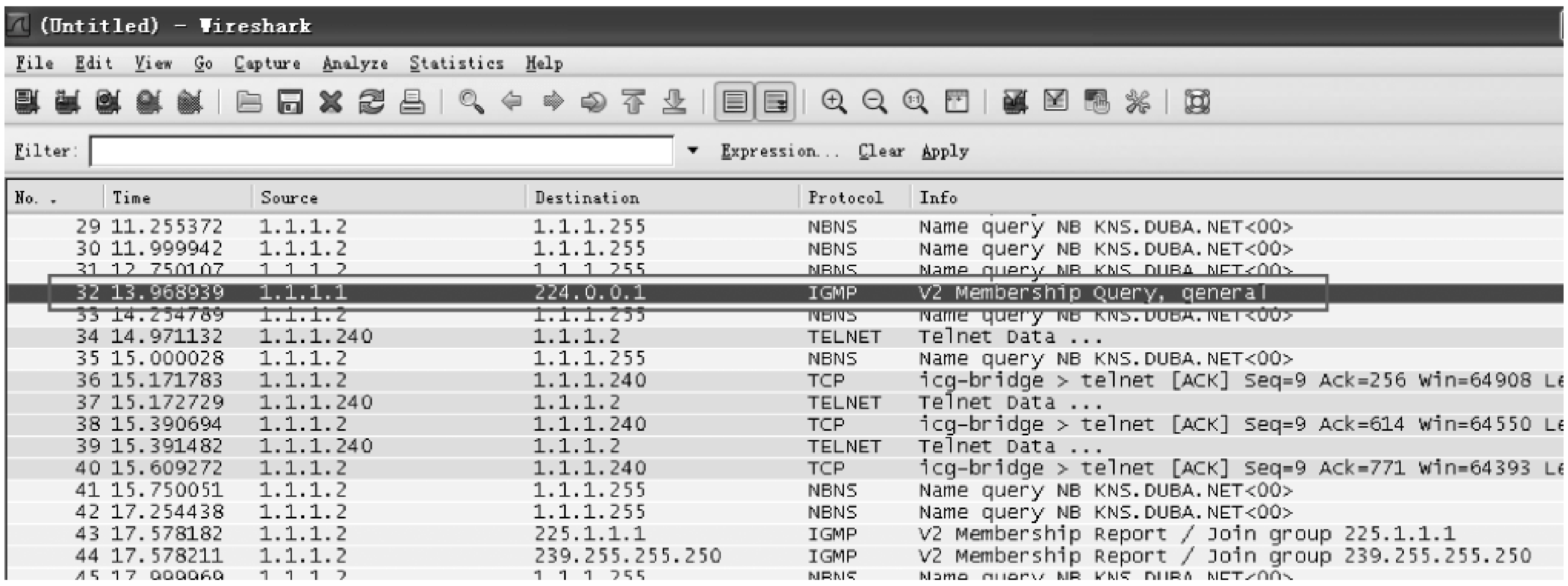
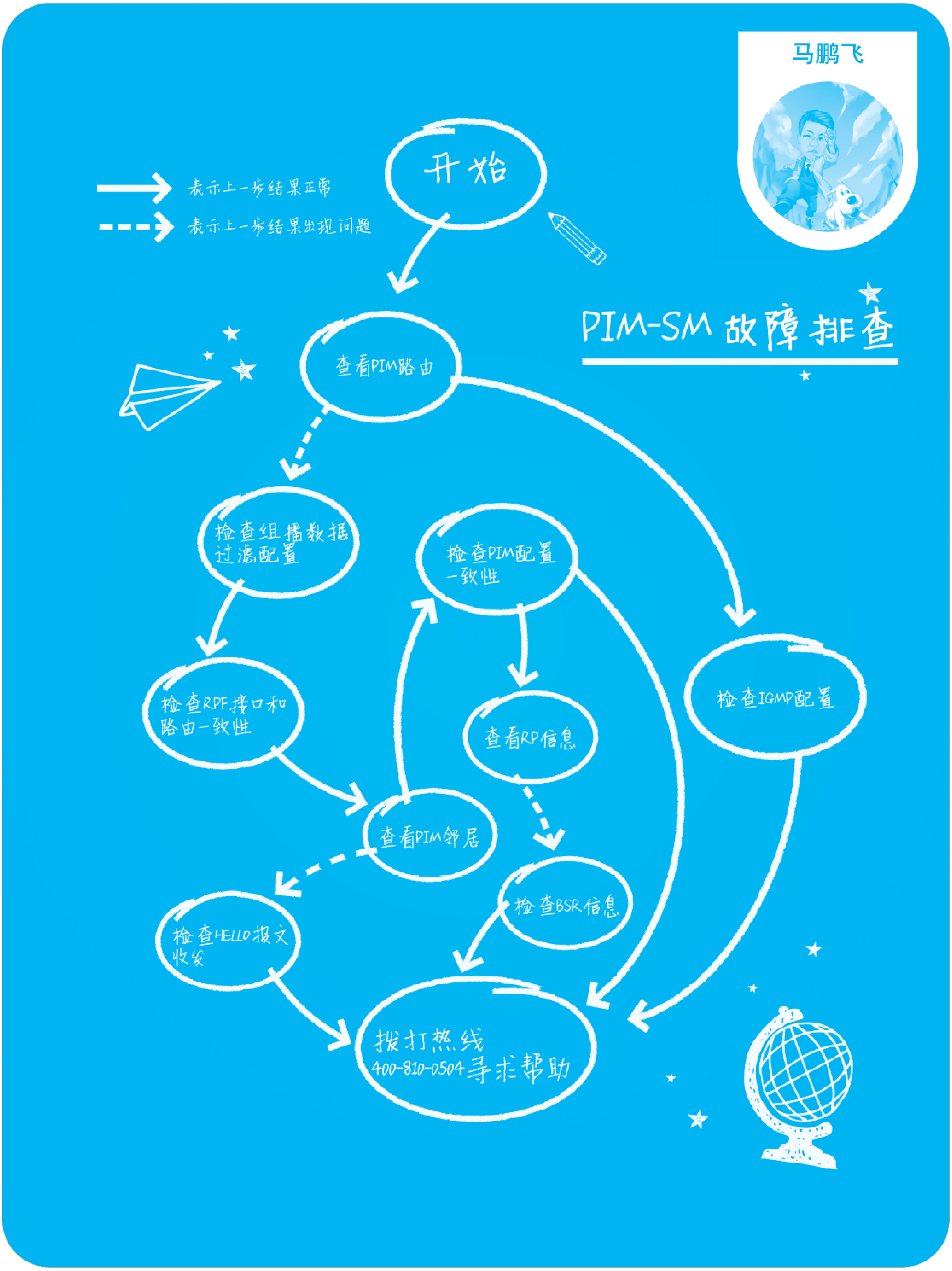


图 1-6　主机抓包对应报文


马鹏飞
表示上一步结果正常
表示上一步结果出现问题
开始
PIM-SM 故障排查
查看PIM路由
检查组播数据过滤配置
检查PIM配置一致性
检查IGMP配置
检查RPF接口和路由一致性
查看RP信息
查看PIM邻居
检查BSR信息
检查HELLO报文收发
拨打热线 400-810-0504 寻求帮助

01 公共协议 ＞ 1.2 IP 组播 ＞ 1.2.3 PIM-SM 故障排查 ＞ 步骤详解

1．开始

组播分为二层和三层组播协议，其中，IGMP-Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组，IGMP 负责 IP 组播成员管理，用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系，PIM-DM 和 PIM-SM 是运行在路由器之间或三层交换机之间的三层组播路由协议，通过单播路由协议产生相应的组播路由表项。

PIM-SM 协议定位故障的思路是：先查路由，再查邻居，最后查 RP/BSR 等配置。

2．查看 PIM 路由

在 PIM-SM 中，RPT 树开始转发报文后，沿途的组播路由器上都会建立对应的(S,G)表项，并且通过查看组播路由表，如果有接收者加入组播组 G，则从 RP 到接收者侧 DR 路径上的路由器会在其转发表中生成一个(＊,G)表项。

命令：***display pim routing-table*** [*group-address*]

例如：通过命令查看当前组播路由表，组播流量经过的所有路由器都有组播组 225.0.0.1 的(S,G)表项存在，从 RP 到接收者侧 DR 路径上的所有路由器都有组播组 225.0.0.1 的(＊,G)和(S,G)表项，且上下游接口信息正确。

```
[H3C]display pim routing-table 225.0.0.1
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.0.0.1)
     RP: 10.1.1.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:02:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface101
             Protocol: igmp, UpTime: 00:02:28, Expires: -

(1.1.1.10, 225.0.0.1)
     RP: 10.1.1.2 (local)
     Protocol: pim-sm, Flag: SPT 2MSDP ACT
     UpTime: 00:05:22
     Upstream interface: Vlan-interface100
         Upstream neighbor: 10.1.1.1
         RPF prime neighbor: 10.1.1.1
Downstream interface(s) information:
   Total number of downstreams: 1
         1: Vlan-interface101
             Protocol: pim-sm, UpTime:  - , Expires:  -
```

3．检查 IGMP 配置

检查在需要建立和维护组播组成员关系的接口上是否使能了 IGMP。

命令：*display current-configuration interface*

```
[H3C]display current-configuration interface
#
interface Vlan-interface101
 ip address 2.1.1.1 255.255.255.0
 igmp enable
#
return
```

4. 检查组播数据过滤配置

检查是否应用了组播数据过滤功能，使能该功能的路由器将按照 ACL 规则对流经自己的组播数据进行过滤，决定是否继续转发组播数据。

例如：通过命令查看，PIM 节点下的过滤配置，有匹配 ACL 规则号 3000 的过滤器，未通过匹配的报文会被丢弃。

命令：PIM 节点下 ***display this***

```
[H3C-pim]display this
#
pim
 source-policy 3000
#
return
```

查看所配置的 ACL 规则，检查是否将所要实现的组播组或邻居进行了过滤。

命令：***display acl*** *acl-number*

例如：只需要过滤 IP 地址为 225.0.0.1 的组播组。

```
[H3C]display acl 3000
Advanced ACL  3000, named -none-, 2 rules,
Statistics is enabled
ACL's

step is 5
 rule 0 deny ip destination 225.0.0.1 0
 rule 5 permit ip
```

5. 检查 RPF 接口和路由一致性

组播数据由直连组播源的第一跳路由器扩散到直连客户端的最后一跳路由器。无论组播数据扩散到哪一台路由器，只有该路由器存在到达组播源的路由，才会创建(S,G)表项，查看组播域内路由器，针对组播源到 RP 的 SPT 树，检查是否有到达组播源的路由，检查 RPF 接口和到达组播源的单播路由的下一跳接口是否一致。针对 RP 到接收者的 RPT 树，检查 RPF 接口和到达 RP 的单播路由的下一跳接口是否一致。

命令：***display ip routing-table*** *ip-address*

例如：通过命令查看，可以确认存在到达组播源的路由 1.1.1.0/24，下一跳是 10.1.1.1，并且查看 PIM 路由表，10.1.1.1 是 RPF 邻居接口。

```
[H3C]display ip routing-table 1.1.1.1
Routing Tables: Public
        Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost        NextHop        Interface

1.1.1.0/24          OSPF   10   2           10.1.1.1       Vlan100

[H3C]display pim routing-table1.1.1.10 225.0.0.1
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

(1.1.1.10, 225.0.0.1)
     RP: 10.1.1.2 (local)
     Protocol: pim-sm, Flag: SPT 2MSDP ACT
     UpTime: 00:05:22
     Upstream interface: Vlan-interface100
         Upstream neighbor: 10.1.1.1
         RPF prime neighbor: 10.1.1.1

Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface101
             Protocol: pim-sm, UpTime:  - , Expires:  -
```

6. 查看 PIM 邻居信息

查看路由器上 PIM 邻居信息,检查 RPF 邻居是否是 PIM 邻居。

命令:*display pim neighbor*

例如:通过命令查看,可以确认两台设备互联网段上存在 PIM 邻居,且是 RPF 邻居。

```
[H3C]display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 1

Neighbor        Interface        Uptime     Expires   Dr-Priority  Mode
 10.1.1.1       Vlan100          07:07:41   00:01:35 1
```

7. 检查 HELLO 报文收发

通过在设备上 debug,检查 PIM Hello 报文是否正常交互。

例如:通过 debugging 命令查看 PIM 邻居交互报文,可以看到正常发出 Hello 报文,也能收到邻居发出的 Hello 报文。

```
<H3C>debugging pim neighbor
<H3C>terminal monitor
Info: Current terminal monitor is on.
<H3C>terminal debugging
Info: Current terminal debugging is on.

[H3C]
*May 30 14:18:17:991 2013 H3C PIM/7/NBR: (public net): PIM ver 2 HEL sending 2.1.1.1 ->
224.0.0.13 on GigabitEthernet3/0/2   (P011695)
```

```
* May 30 14:18:18:011 2013 H3C PIM/7/NBR: (public net): Option: 1, length: 2 (P011730)
...
* May 30 14:18:35:561 2013 H3C PIM/7/NBR: (public net): PIM ver 2 HEL receiving 2.1.1.2 ->
224.0.0.13 on GigabitEthernet3/0/2  (P011695)
* May 30 14:18:35:581 2013 H3C PIM/7/NBR: (public net): Option: 1, length: 2 (P011730)
...
```

8. 检查 PIM 配置一致性

检查 RPF 接口和 RPF 邻居所在路由器的对应接口上是否使能了相同模式的 PIM。

命令：*display pim interface verbose*

例如：通过命令查看，可以确认相关接口下配置了 PIM-SM。

```
[H3C]display pim interface verbose
 VPN-Instance: public net
 Interface: Vlan-interface100, 10.1.1.2
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 10.1.1.2 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
 ...
```

9. 查看 RP 信息

RP 是 PIM-SM 的核心，为特定的组服务。网络中可以同时存在多个 RP。必须保证所有路由器的 RP 信息完全一致，并且对于某个特定的组映射到相同的 RP，否则必然导致组播数据转发异常。如果使用静态 RP 机制，必须在全网所有路由器上配置完全相同的静态 RP 命令。如果通过配置 C-RP，通过自举机制动态选举 RP，则必须保证 C-RP 和 BSR 之间路由可达。

命令：***display pim rp-info*** [*group-address*]

例如：通过命令查看路由器上的 RP 信息，可以看到公网实例中组播组 225.0.0.1 对应的 RP 地址为 10.1.1.1。

```
[H3C]display pim rp-info 225.0.0.1
 VPN-Instance: public net
 BSR RP Address is: 10.1.1.1
     Priority: 192
     HoldTime: 150
     Uptime: 02:38:20
     Expires: 00:02:11
 RP mapping for this group is: 10.1.1.1 (local host)
```

10. 检查 BSR 信息

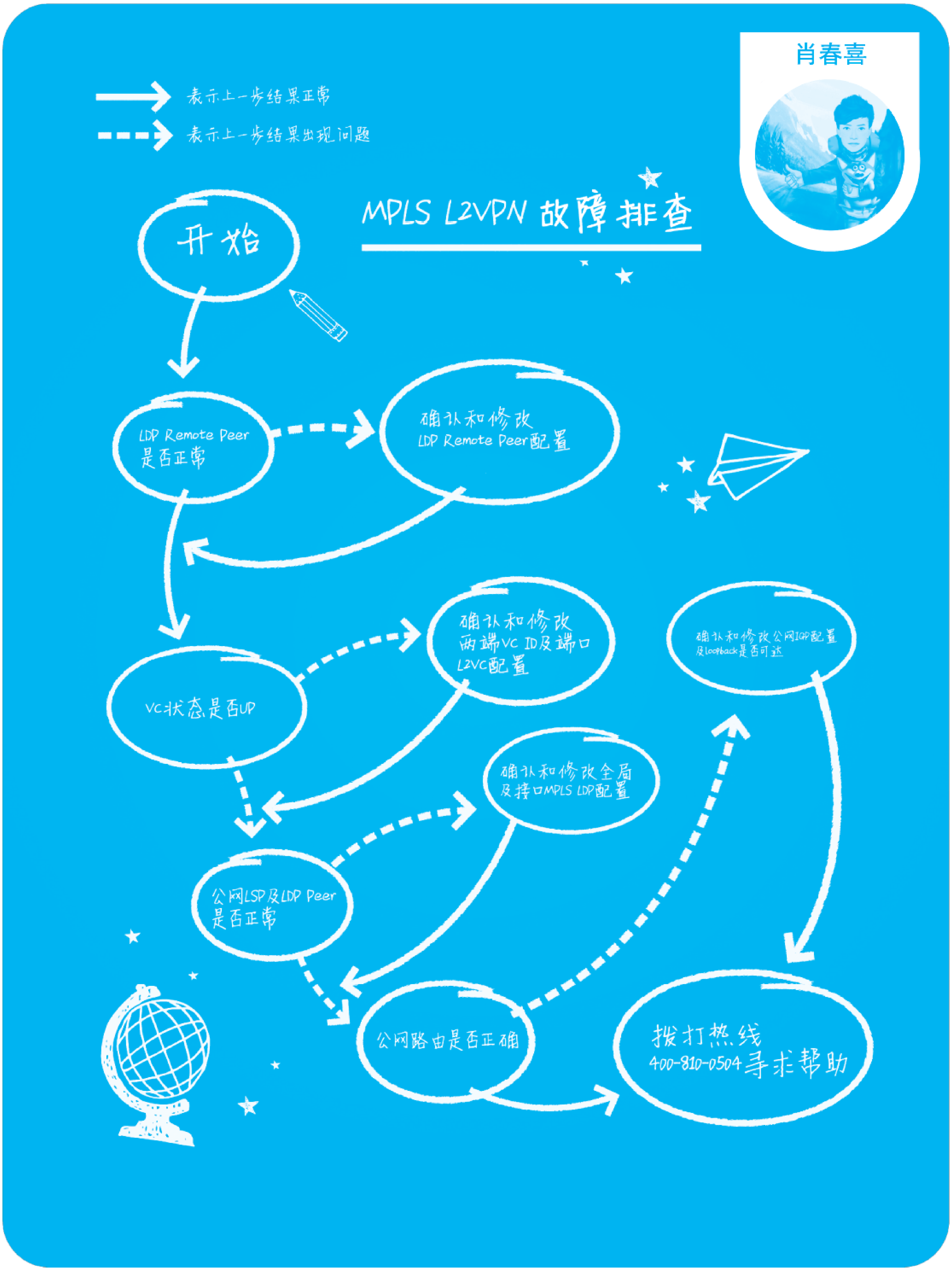
在一个 PIM-SM 域中只能有一个 BSR，但需要配置至少一个 C-BSR。BSR 负责在 PIM-SM 域中收集并发布 RP 信息。

命令：*display pim bsr-info*

例如：通过命令查看当前路由器上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[H3C]display pim bsr-info
 VPN-Instance: public net
 Elected BSR Address: 10.1.1.1
     Priority: 64
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:18:21
     Expires: 00:01:59

 Candidate RP: 10.1.1.2(Vlan-interface100)
     Priority: 192
     HoldTime: 150
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:39
```


肖春喜
表示上一步结果正常
表示上一步结果出现问题
MPLS L2VPN 故障排查
开始
LDP Remote Peer
是否正常
确认和修改
LDP Remote Peer配置
VC状态是否UP
确认和修改
两端VC ID及端口
L2VC配置
确认和修改公网IGP配置
及loopback是否可达
确认和修改全局
及接口MPLS LDP配置
公网LSP及LDP Peer
是否正常
公网路由是否正确
拨打热线
400-810-0504寻求帮助

01 公共协议 〉 1.3 MPLS 〉 1.3.1 MPLS L2VPN 故障排查 〉 步骤详解

1. 开始

由于 MPLSL2VPN 的报文由内层私网 VC 标签和外层公网标签构成，转发主要依赖于外层 LSP。所以定位故障的思路是：先查 VC 标签，再查公网标签；先查远程 LDP Peer，再查本地 LDP Peer。

2. 流程图相关操作说明

（1）查看 LDP Remote Peer 是否正常

查看本端 PE 路由器是否与对端 PE 正确建立远程 LDP Peer 关系。

命令：*display mpls ldp remote-peer*

例如：通过命令查看，可以确认与远端 PE 正确建立 Remote Peer 关系。

```
<H3C>display mpls ldp remote-peer
                         LDP Remote Entity Information
-------------------------------------------------------------------------------
 Remote Peer Name    :1
 Remote Peer IP      :10.10.10.2        LDP ID : 10.10.10.10:0
 Transport Address   : 10.10.10.10

 Configured Keepalive Timer : 45 Sec
 Configured Hello Timer     : 45 Sec
 Negotiated Hello Timer     : 45 Sec
 Hello Message Sent/Rcvd    : 307/304 (Message Count)
 -------------------------------------------------------------------------------
```

（2）确认和修改 LDP Remote Peer 配置

在两端 PE 上创建 ldp remote peer，并配置对端 PE 的 loopback 地址。

例如：本端 PE 上创建 ldp remote peer 1，指定对端 PE 地址为 10.10.10.2，命令为 *mpls ldp remote-peer 1*，*remote-ip 10.10.10.2*。

```
[H3C]display current-configuration
 #
l2vpn
 mpls l2vpn
 #
mpls ldp remote-peer 1
 remote-ip 10.10.10.2
 #
return
```

（3）查看 VC 状态是否 Up

分别查看两端 PE 路由器的 mpls l2vc 连接状态是否 Up，本端和远端 VC Label 是否正确。

命令：*display mpls l2vc*

例如：通过命令查看，可以确认 VC ID 为 101 的 L2VPN 状态是否正常。

```
<H3C>display mpls l2vc
Total ldp vc : 1       1 up        0 down        0 blocked
Transport    Client          Service   VC        Local       Remote
VC ID        Intf            ID        State     VC Label    VC Label
101          S0/2/1          --        Up        1025        1024
```

(4) 确认和修改两端 VC ID 及端口 L2VC 配置

在连接 CE 的端口上配置对端 PE 的 loopback 地址和 VC ID，而且两端 PE 的 VC ID 必须一致。

例如：将本端 PE 的 Serial0/2/1 与对端 PE(10.10.10.2)建立 L2VPN 连接，VC ID 为 101，命令为 *mpls l2vc 10.10.10.2 101*。

```
<H3C>display current-configuration interface Serial0/2/1
#
interface Serial0/2/1
 mpls l2vc 10.10.10.2 101
#
```

(5) 查看公网 LSP 及 LDP PEER 是否正常

查看整个 LSP 上的所有设备是否已经为两个 PE 的 loopback 地址正确的分配了公网标签，以及 LDP Peer 是否正常。

命令：*display mpls lsp*，*display mpls ldp peer*

例如：通过命令查看，可以确认对端 loopback 地址 10.10.10.2/32 的公网标签为 1024，LDP Peer 状态正常。

```
<H3C>display mpls lsp
-------------------------------------------------------------------------------
                  LSP Information: LDP LSP
-------------------------------------------------------------------------------
FEC                  In/Out Label     In/Out IF                  Vrf Name
10.10.10.2/32        NULL/1024        -/S0/2/0

<H3C>display mpls ldp peer
         LDP Peer Information in Public network
 Total number of peers: 2
---------------------------------------------------------------------------------
Peer-ID                  Transport-Address   Discovery-Source
---------------------------------------------------------------------------------
10.10.10.1:0             10.10.10.1          Serial0/2/0
---------------------------------------------------------------------------------
```

(6) 确认和修改全局及接口 MPLS LDP 配置

在两端 PE 上全局开启 MPLS 和 MPLS LDP，并在接口下配置 MPLS 和 MPLS LDP。

例如：本端 PE 上设置 mpls lsr-id 10.10.10.10，全局和接口下开启 MPLS 和 MPLS LDP，命令为 *mpls*，*mpls ldp*。

```
[H3C]display current-configuration
#
```

```
mpls lsr-id 10.10.10.10
#
mpls
#
mpls ldp
#
interface Serial0/2/0
 mpls
 mpls ldp
#
```

（7）查看公网路由是否正确

确认是否在公网 LSP 途径的所有设备上都存在两端 PE 的 loopback 地址精确路由。

命令：*display ip routing-table*

例如：通过命令查看，可以确认本端存在去往对端的公网路由 10.10.10.2/32，下一跳为 192.168.1.2。

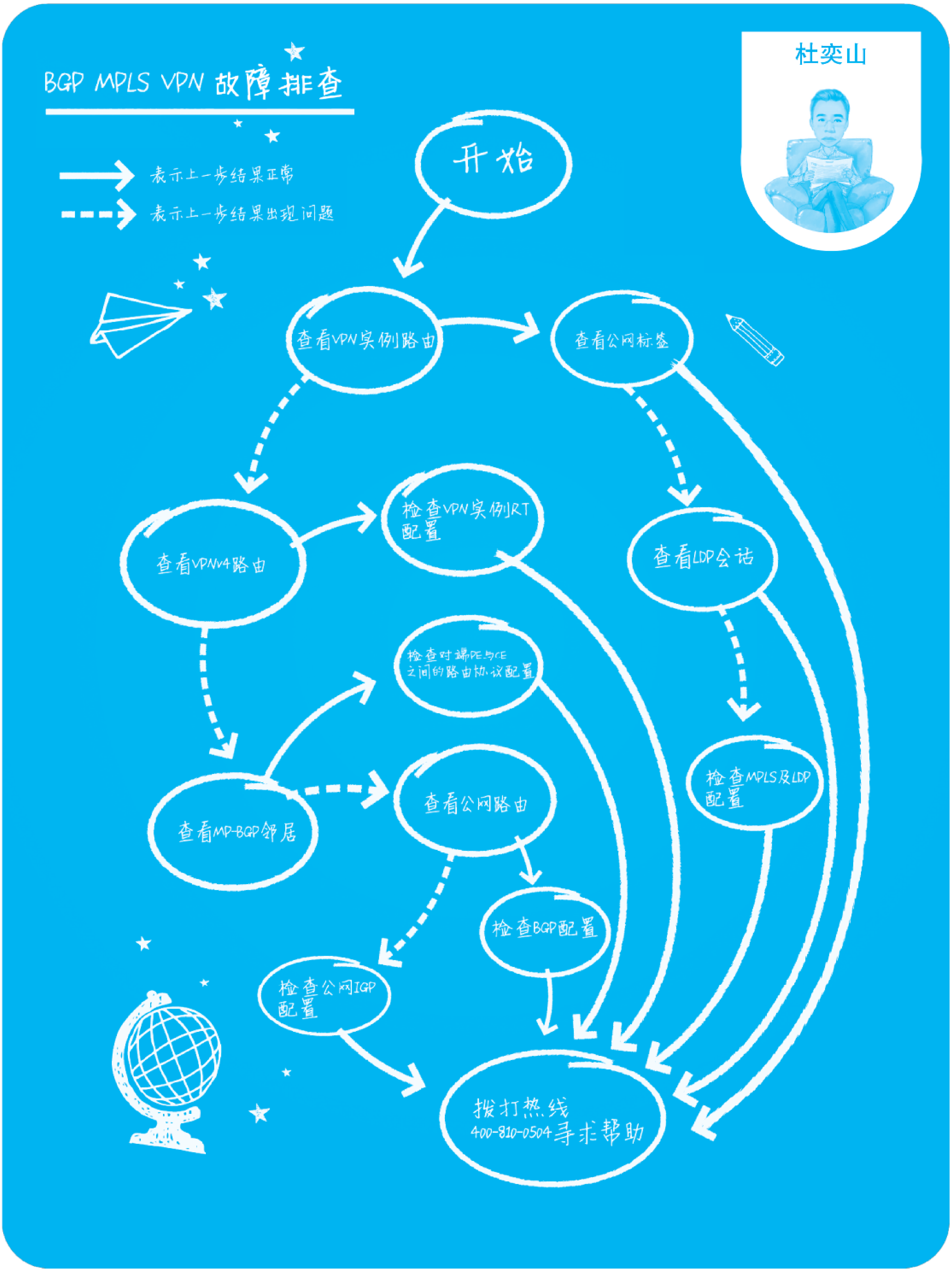
```
<H3C>display ip routing-table
Routing Tables: Public
         Destinations : 9          Routes : 9
Destination/Mask      Proto   Pre   Cost          NextHop         Interface
10.10.10.2/32         OSPF    10    3124          10.10.1.2       S0/2/0
```

（8）确认和修改公网 IGP 配置及 loopback 是否可达

是否通过公网 IGP 将 PE 的 loopback 地址的路由发布出去。

例如：公网 IGP 使用 OSPF 查看 OSPF 配置，确认已将 PE 的 loopback 地址 10.10.10.10 发布进公网 OSPF 内。

```
[H3C]display current-configuration configuration ospf
#
ospf 100
 area 0.0.0.1
  network 10.10.10.10 0.0.0.0
  network 10.10.1.0 0.0.0.255
#
```


杜奕山
BGP MPLS VPN 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看VPN实例路由
查看公网标签
查看VPNv4路由
检查VPN实例RT配置
查看LDP会话
检查对端PE与CE之间的路由协议配置
检查MPLS及LDP配置
查看MP-BGP邻居
查看公网路由
检查BGP配置
检查公网IGP配置
拨打热线 400-810-0504寻求帮助

1. 开始

由于 BGP/MPLS VPN 的报文转发是基于 LSP 的，而 LSP 是依附于路由的。所以定位故障的思路是：先查路由、再查标签；先查私网、再查公网。

2. 流程图相关操作说明

（1）查看 VPN 实例路由

分别查看两端 PE 路由器的 vpn-instance 中是否存在对端 PE 的 VPN 路由。

命令：*dis ip routing-table vpn-instance vpn1 x.x.x.x*（目标地址）

例如：通过命令查看，可以确认存在对端 PE 的 VPN 路由 200.200.200.200/32，下一跳是 3.3.3.3。

```
<H3C>dis ip routing-table vpn-instance vpn1 200.200.200.200
Routing Tables: vpn1
         Destinations : 3          Routes : 3

Destination/Mask      Proto    Pre   Cost        NextHop        Interface
200.200.200.200/32     BGP     255   0            3.3.3.3       NULL0
```

（2）查看 BGP VPNv4 路由

查看本端 PE 路由器的是否已经正确的获得 BGP VPNv4 路由。

命令：*display bgp vpnv4 all routing-table x.x.x.x*（目标地址）

<0-32>/x.x.x.x（网络掩码长度/网络掩码）

例如：通过命令查看，可以确认已获得 VPNv4 路由——200.200.200.200，且私网标签为 1025。

```
<H3C>display bgp vpnv4 all routing-table 200.200.200.200/32

 BGP local router ID : 1.1.1.1
 Local AS number : 100

 Route Distinguisher: 100:1
 Paths:   1 available, 0 best, 1 VPNv4 best

 BGP routing table entry information of 200.200.200.200/32:
 Label information (Received/Applied):1025/NULL
 From              : 3.3.3.3 (3.3.3.3)
 Original nexthop : 3.3.3.3
 Ext-Community    : <RT: 100:1>
 AS-path           : (null)
 Origin            : incomplete
 Attribute value   : MED 0, localpref 100, pref-val 0, pre 255
 State             : valid, internal, VPNv4 best,
 Not advertised to any peers yet
```

(3) 查看 MP-BGP 邻居

确认邻居状态机是否达到 Established 状态。

命令：*display bgp vpnv4 all peer*

例如：通过命令查看，可以确认本端 AS100 内 BGP 邻居 3.3.3.3 状态已为 Established。

```
<H3C>display bgp vpnv4 all peer  3.3.3.3

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Total number of peers : 1                  Peers in established state : 1

  Peer                    AS   MsgRcvd   MsgSent OutQ PrefRcv Up/Down   State

  3.3.3.3                100        17        13    0        1 00:12:36
Established
```

(4) 查看公网路由

确认是否在公网 LSP 途径的所有设备上都存在对端 PE 的 loopback 地址的精确路由(必须是 32 位掩码)。

命令：*display ip routing-table*

例如：通过命令查看，可以确认本端存在去往对端的公网路由 3.3.3.3/32，下一跳为 192.168.1.2。

```
<H3C>display ip routing-table
Routing Tables: Public
        Destinations : 12        Routes : 12

Destination/Mask     Proto    Pre  Cost          NextHop          Interface

3.3.3.3/32             OSPF    10   4686          192.168.1.2      S0/2/0
```

(5) 查看 BGP 配置

确认在 VPNv4 地址族下是否正确配置了 BGP 邻居关系。

命令：*display current-configuration configuration bgp*

例如：

```
<H3C>display current-configuration configuration bgp
#
bgp 100
 undo synchronization
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
#
 ipv4-family vpnv4
  peer 3.3.3.3 enable
#
```

(6) 检查本地 VPN 实例 RT 配置

检查本地 VPN 实例配置中 RT 是否配置匹配。

命令：*display this*(VPN 实例地址族下执行)

```
[H3C-vpn-instance-vpn1] display this
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
 #
 return
```

(7) 检查对端 PE 与 CE 之间的路由协议

查看对于每个 vpn-instance,是否将该 vpn-instance 的路由引入到 MP-BGP 中。

命令：*display this*(BGP 视图下)

例如：将 vpn-instance vpn1 的 OSPF 路由引入到 MP-BGP 中。

```
[H3C-bgp] display this
#
bgp100
peer1.1.1.1 as-number 100
#
 ipv4-family vpn-instance vpn1
 import-route ospf 100
#
```

(8) 检查公网 IGP 配置

是否通过公网 IGP 将 PE 的 loopback 地址的路由发布出去。

命令：*display current-configuration configuration ospf*

例如：公网 IGP 使用 OSPF,查看 OSPF 配置,可以确认已将 PE 的 loopback 地址 1.1.1.1 发布进公网 OSPF 内。

```
[H3C]display current-configuration configuration ospf
#
ospf 1
area 0.0.0.0
  network 1.1.1.1 0.0.0.0
#
return
```

(9) 查看公网标签

查看整个 LSP 上的所有设备是否已经为两个 PE 的 loopback 地址正确的分配了公网标签。

命令：*display mpls lsp include x.x.x.x*(目标地址) <*0-32*>(网络掩码长度)

例如：通过命令查看,可以确认已正确分配公网标签 1026。

```
<H3C>display mpls lsp include 3.3.3.3 32
------------------------------------------------------------------------------
                    LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label     In/Out IF                       Vrf Name
3.3.3.3/32          NULL/1026        -/S0/2/0
```

(10) 查看 LDP 会话关系

查看两台相邻的 PE 或 P 路由器之间是否正确建立了 LDP 邻居会话关系。

命令：*display mpls ldp session x.x.x.x*

例如：通过命令查看，可以确认本端已存在 LDP 邻居 3.3.3.3:0。

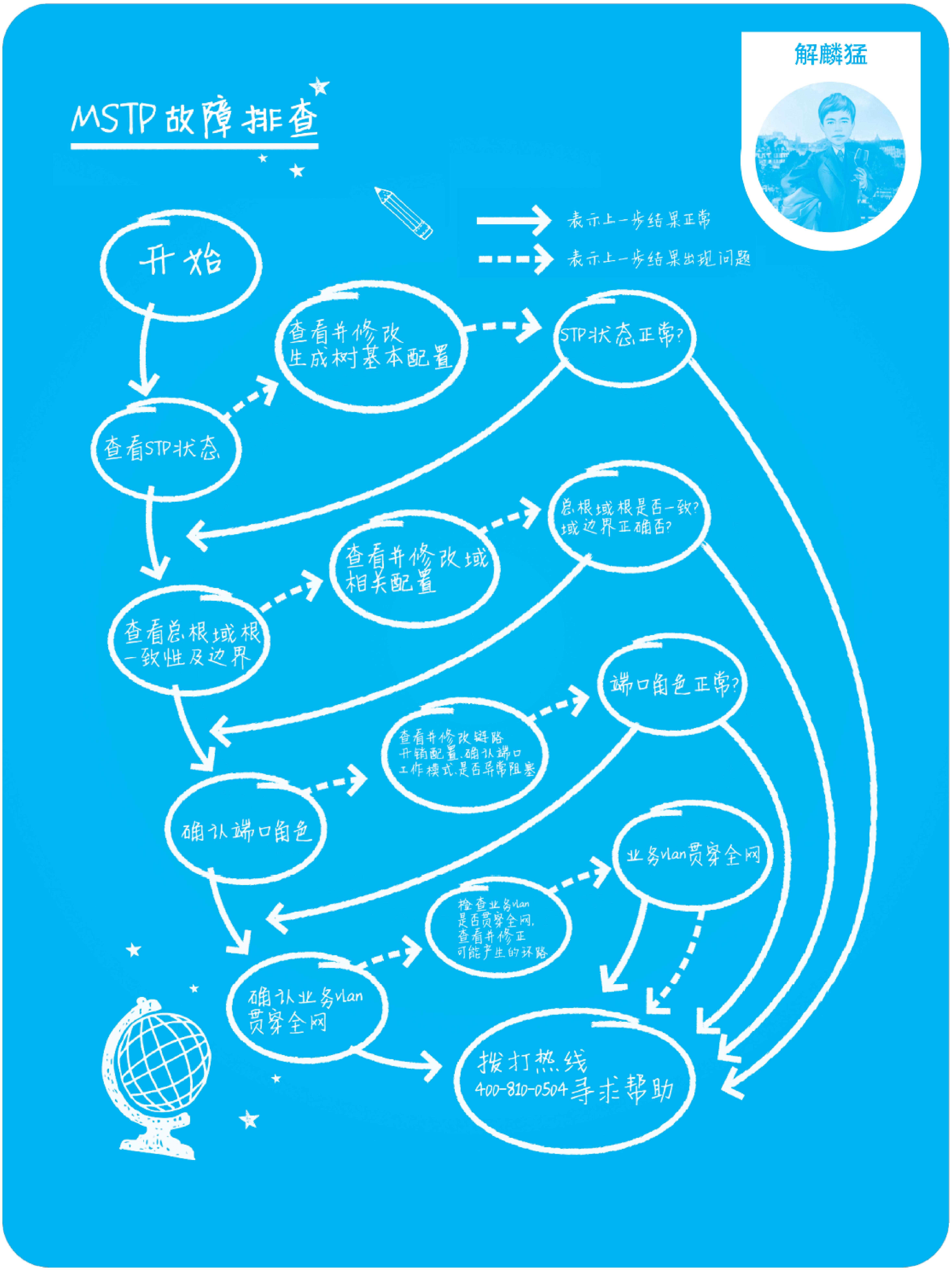
```
<H3C>display mpls ldp session 3.3.3.3

              LDP Session(s) in Public Network
 Total number of sessions: 2
 ------------------------------------------------------------------------
 Peer-ID          Status        LAM   SsnRole   FT    MD5   KA-Sent/Rcv
 ------------------------------------------------------------------------
 3.3.3.3:0        Operational   DU    Passive   Off   Off     318/319
```

(11) 检查 MPLS 及 LDP 配置

查看该设备是否在全局使能了 MPLS 和 LDP，以及在相应的接口上使能了 LDP。

命令：*display current-configuration*


解麟猛
MSTP故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看STP状态
查看并修改
生成树基本配置
STP状态正常?
查看总根域根
一致性及边界
查看并修改域
相关配置
总根域根是否一致?
域边界正确否?
确认端口角色
查看并修改链路
开销配置，确认端口
工作模式，是否异常阻塞
端口角色正常?
确认业务vlan
贯穿全网
检查业务vlan
是否贯穿全网，
查看并修正
可能产生的环路
业务vlan贯穿全网
拨打热线
400-810-0504寻求帮助

1. 开始

MSTP 定位故障的思路是按照生成树的工作原理：先确定二层网络 MSTP 的运行范围，再确定全网根桥及域根的一致性，确认域边界，然后再确定每一台参与 MSTP 计算的网桥的端口角色是否正确，包括在 CIST 和 MSTI 中的端口角色是否正确，最后再确定各类生成树保护机制是否导致了异常端口阻塞，业务 VLAN 是否贯穿全网，是否存在可能的环路。

2. 流程图相关操作说明

(1) 查看生成树状态

大量的交换机默认情况下并不开启生成树协议，因此要确认每一台网桥都开启了生成树功能并且生成树协议模式为 MSTP。

命令：*display stp*

例如：通过命令查看正确的结果。

```
<H3C>display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge          :32768.0023-8939-88b0
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
```

通过命令查看错误的结果。

```
<H3C>disp stp
 Protocol Status     :disabled
 Protocol Std.       :IEEE 802.1s
 Version             :3
```

(2) 查看并修改生成树基本配置

生成树的基本配置包括四项，所有参与生成树计算的网桥务必保持一致。

命令：*display current-configuration*

例如：通过命令查看配置。

```
<H3C>display current-configuration
 #
   stp enable                    //使能生成树
 #
```

① 生成树模式为 MSTP。

[H3C]*stp mode mstp*

MSTP 为默认模式，配置不显示。

② 生成树的网络直径。

[H3C] *stp bridge-diameter diameter*

不建议进行配置，使用默认参数 7，配置不显示。

③ 生成树的时间参数。

[H3C]*stp timer*

不建议进行配置，使用默认参数，配置不显示。

(3) 查看根桥及域根的一致性，确定域边界

查看整个二层网络中相关网桥的总根桥必须为同一个网桥，在同一个域内每个 MSTI 的域根为同一个网桥。

命令：*display stp*

例如：通过命令查看根桥的结果。

```
<H3C>display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.0023-8914-3ea9
Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0.0023-8939-88b0 / 20
CIST RegRoot/IRPC   :32768.0023-8914-3ea9 / 0
<H3C>display stp instance 2
-------[MSTI 2 Global Info]-------
MSTI Bridge ID      :4096.0023-8914-3ea9
MSTI RegRoot/IRPC   :0.0023-8927-adf5 / 20
```

要求所有网桥查询到的总根桥必须一致，同一域内的同一 MSTI 的域根也需要一致，确定域边界。

在域边界联往总根桥的接口状态查询。

命令：*<H3C>display stp interface GigabitEthernet 1/0/2*

```
<H3C>display stp interface GigabitEthernet 1/0/2
----[CIST][Port2(GigabitEthernet1/0/2)][FORWARDING]----
 Port Protocol        :enabled
 Port Role            :CIST Root Port
 ----[MSTI 1][Port2(GigabitEthernet1/0/2)][FORWARDING]----
 Port Role            :Master Port
 ----[MSTI 2][Port2(GigabitEthernet1/0/2)][FORWARDING]----
 Port Role            :Master Port
<H3C>display stp interface GigabitEthernet 2/0/2
----[CIST][Port91(GigabitEthernet2/0/2)][DISCARDING]----
 Port Protocol        :enabled
 Port Role            :CIST Alternate Port
----[MSTI 1][Port91(GigabitEthernet2/0/2)][DISCARDING]----
 Port Role            :Alternate Port
----[MSTI 2][Port91(GigabitEthernet2/0/2)][DISCARDING]----
 Port Role            :Alternate Port
```

(4) 查看各网桥互联接口配置

如果出现网桥总根桥不一致的情况，需要查看根桥不一致的两个相邻网桥互联端口状态及配置。

① 确认端口 STP 处于使能状态。

命令：*display stp interface*

例如：

```
<H3C>display stp interface GigabitEthernet1/0/1

----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol          :enabled
```

② 确认端口未处于单通状态。对于域内互联的两个接口，通过显示接口的 BPDU 收发报文，如果两端口都在发，其中只有一端收到，则说明存在单通现象。

对于域间互联的两个接口，通过显示接口的 BPDU 收发报文，正常情况下应该是一端发，一端收，且发送 BPDU 的端口应该有学习到的动态 MAC。如果相连的两端口都在发送 BPDU，则说明存在单通现象。

```
<H3C>display stp interfaceGigabitEthernet1/0/1
----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
-----------------------------------------------------------------------
BPDU Sent              :2199
           TCN: 0, Config: 0, RST: 0, MST: 2199
BPDU Received          :2295
           TCN: 0, Config: 0, RST: 0, MST: 2295
```

③ 确认端口上配置未启用和 BPDU 相关的过滤功能。

命令：[*H3C*]*display current-configuration interface GigabitEthernet 1/0/1*

④ 如果两交换机之间还联有其他二层设备（如 IPS、FW、传输设备等），需要确保该二层设备透传 BPDU 报文。可以在交换机两边对应的端口上启动 debug 功能，判断收发 BPDU 报文是否一致。

命令：<*H3C*>*debug stp packet interface GigabitEthernet 1/2/0/18 verbose*

例如：

```
<H3C> debug stp packet interface GigabitEthernet 1/2/0/18 verbose
 *Jun 14 00:02:34:606 2013 H3C MSTP/7/PKT: -Chassis=1-Slot=2;
Port114(GigabitEthernet1/2/0/18) Send Mstp-legacy Packet(Length: 103)
00 00 03 02 6c 00 00 00 23 89 14 3e a9 00 00 00
14 80 00 00 23 89 bd a1 8a 80 72 01 00 0c 00 02
00 09 00 00 00 00 40 30 30 32 33 38 39 62 64 61
31 38 61 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 ac 36 17 7f 50 28 3c
d4 b8 38 21 d8 ab 26 de 62 80 00 00 23 89 bd a1
8a 00 00 00 00 14 00 u d a
```

⑤ 如果同一个 MSTP 域被意外分割成多个域，需要查询 MSTP region 配置。

命令：[*H3C*]*display current-configuration*

```
 #
stp region-configuration
 region-name test              //同一域内交换机配置 region-name 必须相同
 instance 1 vlan 100           //实例与 vlan 的映射关系必须相同
 instance 2 vlan 200
 active region-configuration   //修改配置后必须重新执行此命令，使修改生效
 #
```

如若与友商进行 MSTP 互通，需要在和友商互联接口上配置摘要侦听功能。

命令：*stp config-digest-snooping*

（5）确认端口角色

确认相关网桥上相关端口角色是否正常。对于 MSTP 来说，同一个端口在不同的 MSTI 中角色很可能不同。

重点是排查出现故障的相关 vlan（不论是断路还是环路）所经过的路径的相关端口在对应的 MSTI 中角色是否与预期一致。

命令：*[H3C]display stp interface GigabitEthernet2/0/1*

如下命令中显示，端口 2/0/1 在 CIST 中作为根端口，在 MSTI1 中作为根端口，而在 MSTI2 中作为指定端口。

```
[H3C]display stp interface GigabitEthernet 2/0/1
----[CIST][Port90(GigabitEthernet2/0/1)][FORWARDING]----
 Port Protocol         :enabled
 Port Role             :CIST Root Port
----[MSTI 1][Port90(GigabitEthernet2/0/1)][FORWARDING]----
 Port Role             :Root Port
----[MSTI 2][Port90(GigabitEthernet2/0/1)][FORWARDING]----
 Port Role             :Designated Port
```

（6）查看并修改链路开销标准，确认接口工作模式，确定异常阻塞端口

① 查看网桥上 stp 链路开销标准的配置是否一致，正确选路的前提是全网标准一致。

H3C 交换机支持 dot1d、dot1t 和 legacy 三种标准。默认是 legacy 标准，属于 H3C 公司私有。和友商进行互通时建议使用 dot1t 标准。

命令：*display stp*

例如：通过命令查看，可以确认本网桥选用的 stp 链路开销标准。

```
[H3C]display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge            :32768.0023-8927-adf5
Bridge Times           :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC         :0.0023-8939-88b0 / 20
CIST RegRoot/IRPC      :32768.0023-8914-3ea9 / 20
CIST RootPortId        :128.90
BPDU-Protection        :disabled
Bridge Config-
Digest-Snooping        :disabled
TC or TCN received     :47
Time since last TC     :0 days 0h:7m:48s

----[Port90(GigabitEthernet2/0/1)][FORWARDING]----
 Port Protocol         :enabled
 Port Role             :CIST Root Port
 Port Priority         :128
 Port Cost(Legacy)     :Config=auto / Active=20
```

修改 stp 链路开销标准命令：[H3C]*stp pathcost-standard dot1t*

② 查看相关网桥互联接口的工作模式（速度和双工模式），确认工作在预设定状态。

命令：*display interface GigabitEthernet 1/0/1*

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8939-88d2
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair, Port hardware type is 1000_BASE_T
 1000Mbps-speed mode, full-duplex mode
```

③ 查看是否有相关端口处于异常阻塞状态。如果端口处在异常阻塞状态，说明网络曾经发生过异常。异常阻塞通常与生成树的几种保护机制相关。

以下为根保护机制导致的端口异常阻塞。

命令：*display stp interface GigabitEthernet 1/0/1*

```
[H3C-GigabitEthernet1/0/1]display stp interface GigabitEthernet 1/0/1
----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol          :enabled
 Port Role              :CIST Designated Port
 Protection Type        :Root
  ----[MSTI 1][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Role              :Designated Port
  ----[MSTI 2][Port1(GigabitEthernet1/0/1)][DISCARDING]----
 Port Role              :Designated Port
 [H3C-GigabitEthernet1/0/1]
```

从端口统计上看，端口在 MSTI2 中的角色是 Designated Port，但出于 DISCARDING 状态，属于异常阻塞。再看保护类型属于根保护，初步判断是有更高优先级的网桥连接所致。

查看历史告警记录。

命令：*<H3C>display logbuffer reverse*

```
<H3C>display logbuffer  reverse
#Apr 26 14:31:17:544 2000 H3C MSTP/1/RGSUp: hwPortMstiRootGuarded: Instance 2's

ROOT-Protection port 2.9437184 received superior message!
%Apr 26 14:31:17:714 2000 H3C MSTP/4/MSTP_ROOT_PROTECTION:Instance 2's

ROOT-Protection port GigabitEthernet1/0/1 received superior BPDUs.
```

从告警记录上看，确实在 MSTI2 中收到了更高优先级 BPDU 导致 MSTI2 中的报文转发状态处于 DISCARDING 状态。

以下为环路保护导致的端口异常阻塞。

```
[H3C]display stp interface GigabitEthernet 1/0/1
----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol          :enabled
 Port Role              :CIST Designated Port
Protection Type         :Loop
----[MSTI 1][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Role              :Designated Port
```

```
----[MSTI 2][Port1(GigabitEthernet1/0/1)][DISCARDING]----
 Port Role                :Designated Port
```

告警信息：

```
<H3C>disp logbuffer   reverse
#Apr 26 14:40:37:641 2000 H3C MSTP/1/LGEXP: hwPortMstiLoopGuarded: Instance 2's

LOOP-Protection port 2.9437184 did not receive message!
%Apr 26 14:40:37:811 2000 H3C MSTP/5/MSTP_BPDU_RECEIVE_EXPIRY: Instance 2's

Port GigabitEthernet1/0/1 received no BPDU within the rcvdInfoWhile interval. Information of the port
aged out.
%Apr 26 14:40:38:042 2000 H3C MSTP/6/MSTP_DISCARDING:Instance 2's

GigabitEthernet1/0/1 has been set to discarding state.
%Apr 26 14:40:38:192 2000 H3C MSTP/4/MSTP_LOOP_PROTECTION: Instance 2's

LOOP-Protection port GigabitEthernet1/0/1 failed to receive configuration BPDUs
```

以下为 BPDU 保护导致的端口异常 Down 状态。

```
[H3C]display stp interface GigabitEthernet 1/0/2

----[CIST][Port2(GigabitEthernet1/0/2)][Down]----
 Port Protocol            :enabled
 Port Role                :CISTDisabled Port
 Port Priority            :128
 Port Edged               :Config=enabled / Active=enabled
 BPDU-Protection          :enabled
```

告警信息：

```
#Apr 29 12:16:27:266 2000 H3C MSTP/1/IVBPDU:hwPortMstiBpduGuarded: BPDU-Protection
port 2 received BPDU packet!
%Apr 29 12:16:27:406 2000 H3C MSTP/2/IVBPDU:BPDU-Protection port GigabitEthernet1/0/2
received BPDU packet!
%Apr 29 12:16:27:536 2000 H3C IFNET/4/LINK UPDOWN:
GigabitEthernet1/0/2: link status is Down
```

以下为单端口环路导致的端口异常 DISCARDING 状态。

```
[H3C-GigabitEthernet1/0/2]disp stp int gi 1/0/2

----[CIST][Port2(GigabitEthernet1/0/2)][DISCARDING]----
Port Protocol            :enabled
Port Role                :CISTDesignated Port
Port Edged               :Config=enabled / Active=disabled
Protection Type          :None
```

告警信息：

```
%Apr 29 13:37:54:227 2000 H3C MSTP/2/PDISC:Instance 0's

GigabitEthernet1/0/2 has been set to discarding state!
%Apr 29 13:37:54:368 2000 H3C DRVDBG/4/LOG Info:
Loopback does exist on port GigabitEthernet1/0/2 vlan 1, please check it
```

(7) 检查业务 VLAN 是否贯穿全网(仅指该业务 vlan 需要覆盖到的网桥)

查看出现故障的业务 vlan，进行端到端的全部路径的查询。其中，在 MSTP 域内需要根据对应的 MSTI 进行路径查询。需要确认以下内容。

① 转发路径上每一个端口(网桥互连端口)上正确配置了相应的业务 VLAN。

命令：[H3C]*display interface GigabitEthernet 1/0/1*

```
[H3C]display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
 PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing   : 1(default vlan), 100-110
  VLAN permitted: 1(default vlan), 100-110
  Trunk port encapsulation: IEEE 802.1q
```

② 转发路径上每一个端口(网桥互连端口)上正确学习到了相关 MAC，且多次查看 MAC 是否频繁迁移。

命令：[H3C] *display mac-address xxxx-xxxx-xxxx*

```
[H3C]display mac-address 0000-0000-0021
MAC ADDR         VLAN ID   STATE         PORT INDEX              AGING TIME(s)
0000-0000-0021   100       LEARNED       GigabitEthernet1/0/2    AGING
  ---  1 MAC address(es) found  ---
[H3C]display mac-address 0000-0000-0021
MAC ADDR         VLAN ID   STATE         PORT INDEX              AGING TIME(s)
0000-0000-0021   100       LEARNED       GigabitEthernet1/0/1    AGING

  ---  1 MAC address(es) found  ---
[H3C]
```

如果存在频繁的业务 MAC 飘移，则很可能存在环路问题。需要进行环路的追踪。追踪的原则是判断业务 MAC 正常情况下应该从哪个端口收到，那么从其他的端口收到则可能是环路的端口。通常用 display 看到的端口就是发生环路的端口。

③ 查看转发路径上每一个端口(网桥互连端口)上的流量统计情况，重点关注端口收发报文占用带宽的百分比，组播和广播流量大小。

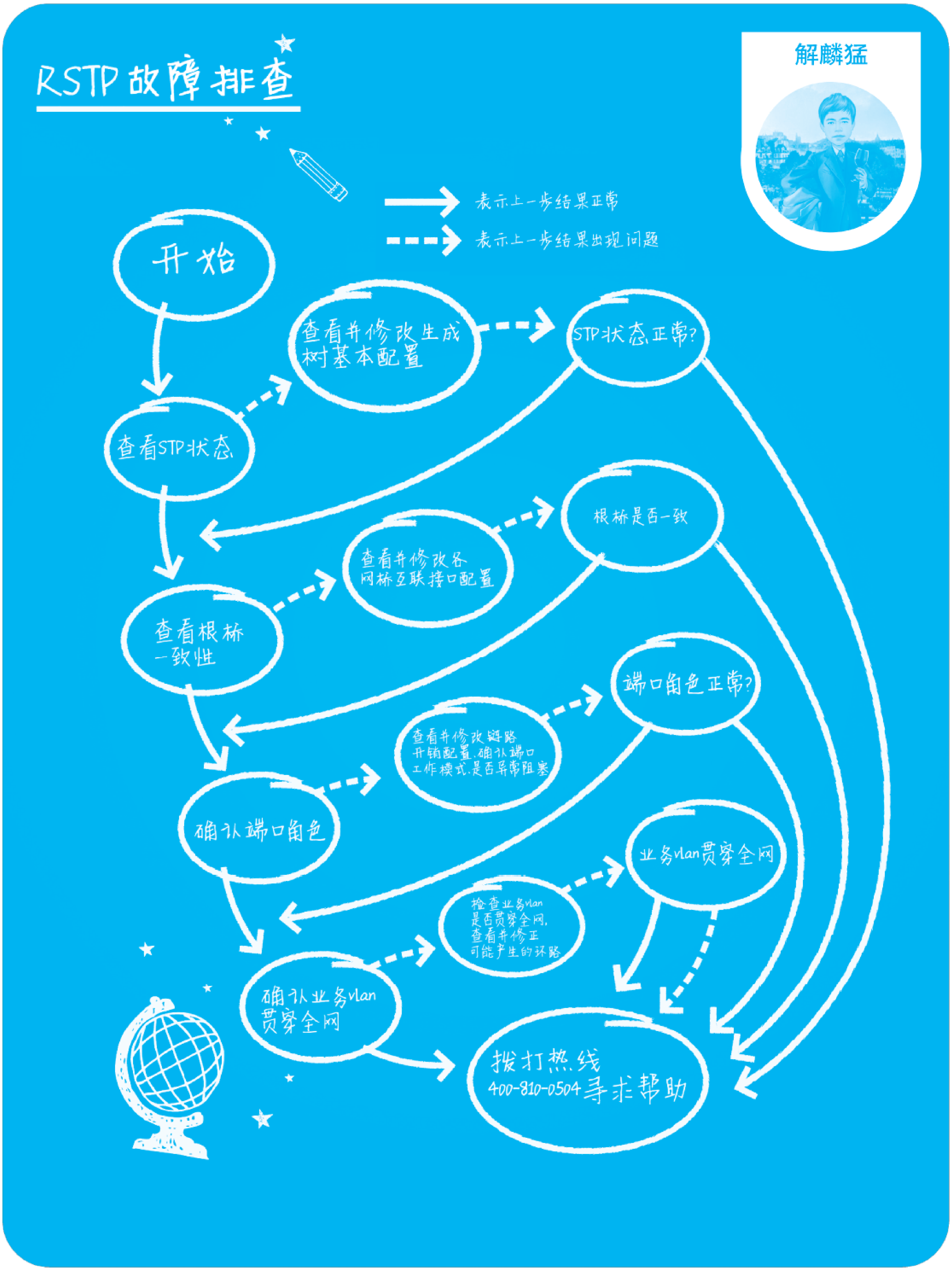
命令：[H3C]*display interface GigabitEthernet 1/0/1*

```
[H3C]display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
Port priority: 0
 Peak value of input: 108553678 bytes/sec, at 2000-04-29 07:15:01
 Peak value of output: 108553647 bytes/sec, at 2000-04-29 07:15:01
```

```
Last 300 seconds input:   822376 packets/sec 108553662 bytes/sec          100%
Last 300 seconds output:   822375 packets/sec 108553630 bytes/sec         100%
Input (total): 453736361 packets, 59892409109 bytes
          0 unicasts, 453604531 broadcasts, 131834 multicasts
Input (normal):   453736365 packets, 59892409109 bytes
          0 unicasts, 453604531 broadcasts, 131834 multicasts
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, 0 parity errors
Output (total): 453585222 packets, 59873409459 bytes
          0 unicasts, 453579906 broadcasts, 5326 multicasts, 0 pauses
Output (normal): 453585232 packets, 59873409459 bytes
          0 unicasts, 453579906 broadcasts, 5326 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, 0 no carrier

[H3C]
```

从端口统计数据看出，如果端口收发数据的百分比超过 90%，并且广播和组播数据占据绝大部分比例时，很可能存在环路。需要追踪此类端口来判断环路路径。判断方式是在环路路径上的端口收发的广播/组播数据量都很大，未在环路路径上的端口仅发方向的广播/组播流量大。


RSTP故障排查
解麟猛
表示上一步结果正常
表示上一步结果出现问题
开始
查看STP状态
查看并修改生成树基本配置
STP状态正常?
查看根桥一致性
查看并修改各网桥互联接口配置
根桥是否一致
确认端口角色
查看并修改链路开销配置,确认端口工作模式,是否异常阻塞
端口角色正常?
确认业务vlan贯穿全网
检查业务vlan是否贯穿全网,查看并修正可能产生的环路
业务vlan贯穿全网
拨打热线
400-810-0504寻求帮助

1. 开始

RSTP 定位故障的思路是按照生成树的工作原理：首先确定二层网络 RSTP 的运行范围，其次确定全网根桥的一致性，再次确定每一台参与 RSTP 计算的网桥的端口角色是否正确，最后再确定各类生成树保护机制是否导致了异常端口阻塞，业务 VLAN 是否贯穿全网，是否存在可能的环路。

2. 流程图相关操作说明

(1) 查看生成树状态

确认每一台网桥都开启了生成树功能并且生成树协议模式为 RSTP。

命令：*display stp*

例如：通过命令查看正确的结果是：

```
<H3C>display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :32768.0023-8939-88b0
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
```

通过命令查看错误的结果是：

```
<H3C>display stp
 Protocol Status     :disabled
 Protocol Std.       :IEEE 802.1s
 Version             :3
```

(2) 查看并修改生成树基本配置

生成树的基本配置包括四项，所有参与生成树计算的网桥务必保持一致。

命令：*display current-configuration*

例如：通过命令查看配置。

```
<H3C>display current-configuration
#
 stp mode rstp                //生成树模式为 RSTP
 stp enable                   //使能生成树
#
```

① 生成树的网络直径。

[H3C] *stp bridge-diameter diameter*

不建议进行配置，使用默认参数。

② 生成树的时间参数。

[H3C] *stp timer*

不建议进行配置，使用默认参数。

(3) 查看根桥的一致性

查看整个二层网络中相关网桥的根桥必须为同一个网桥。

命令：*display stp*

例如：通过命令查看根桥的结果。

```
<H3C>display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge          :32768.0023-8939-88b0
Bridge Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :0.0023-8914-3ea9 / 20
```

要求所有网桥查询到的根桥必须一致。

(4) 查看各网桥互联接口配置

如果出现网桥根桥不一致的情况，需要查看根桥不一致的两个相邻网桥互联端口状态及配置。

① 确认端口 STP 处于使能状态。

命令：*display stp interface GigabitEthernet 1/0/1*

例如：

```
<H3C>display stp interface GigabitEthernet 1/0/1

----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol         :enabled
```

② 确认端口未处于单通状态。通过显示接口的 BPDU 收发报文，正常情况下应该是一端发、一端收，且发送 BPDU 的端口应该有学习到的动态 MAC。如果相连的两端口都在发送 BPDU，则说明存在单通现象。

命令：*display stp interface GigabitEthernet 1/0/1*

```
<H3C>display stp interface GigabitEthernet 1/0/1
----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
------------------------------------------------------------------------
BPDU Sent              :1152
          TCN: 0, Config: 0, RST: 1137, MST: 15
BPDU Received          :39568
          TCN: 0, Config: 0, RST: 39562, MST: 6
```

③ 确认端口上配置未启用和 BPDU 相关的过滤功能。

命令：*[H3C]display current-configuration interface GigabitEthernet 1/0/1*

④ 如果两交换机之间还联有其他二层设备(如 IPS、FW、传输设备等)，需要确保该二层设备透传 BPDU 报文。

可以在交换机两边对应的端口上启动 debug 功能，判断收发 BPDU 报文是否一致。

命令：*<H3C>debug stp packet interface GigabitEthernet 1/2/0/18 verbose*

例如：

```
<H3C> debug stp packet interface GigabitEthernet 1/2/0/18 verbose
 *Jun 13 23:38:26:540 2013 H3C MSTP/7/PKT: -Chassis=1-Slot=2;
```

```
Port114(GigabitEthernet1/2/0/18) Send Rstp Packet(Length: 36)
00 00 02 02 2c 00 00 00 23 89 14 3e a9 00 00 00
14 80 00 00 23 89 bd a1 8a 80 72 01 00 0c 00 02
00 09 00 00
```

(5) 确认端口角色

确认相关网桥上相关端口角色是否正常。

重点是排查出现故障的相关 vlan(不论是断路还是环路)所经过的路径的相关端口角色是否与预期一致。

命令：*display stp interface GigabitEthernet1/0/1*

例如：通过命令查看，该端口目前角色(root port)及所处状态(FORWARDING)。

```
<H3C> display stp interface GigabitEthernet1/0/1
----[CIST][Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol          :enabled
 Port Role              :CIST Root Port
 Port Priority          :128
 Port Cost(Legacy)      :Config=auto / Active=20
 Desg. Bridge/Port      :0.0023-8914-3ea9 / 128.2
```

(6) 查看并修改链路开销标准，确认接口工作模式，确定异常阻塞端口

① 查看网桥上 stp 链路开销标准的配置是否一致，正确选路的前提是全网标准一致。H3C 交换机支持 dot1d、dot1t 和 legacy 三种标准。默认是 legacy 标准，属于 H3C 公司私有，和友商进行互通时建议使用 dot1t 标准。

命令：[*H3C*]*display stp*

例如：通过命令查看，可以确认本网桥选用的 stp 链路开销标准。

```
[H3C]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge            :32768.0023-8939-88b0
Bridge Times           :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC         :0.0023-8914-3ea9 / 20
CIST RegRoot/IRPC      :32768.0023-8939-88b0 / 0
CIST RootPortId        :128.1
BPDU-Protection        :disabled
Bridge Config-
Digest-Snooping        :disabled
TC or TCN received     :30
Time since last TC     :0 days 20h:42m:42s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol         :enabled
 Port Role             :CIST Root Port
 Port Priority         :128
 Port Cost(Legacy)     :Config=auto / Active=20
```

修改 stp 链路开销标准命令：[H3C]*stp pathcost-standard dot1t*

② 查看相关网桥互联接口的工作模式(速度和双工模式),确认工作在预设定状态。

命令:<H3C> *display interface Gigabitethemet 1/0/1*

```
<H3C>display interface Gigabitethernet1/0/1
 GigabitEthernet1/0/1 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8939-88d2
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair, Port hardware type is 1000_BASE_T
 1000Mbps-speed mode, full-duplex mode
```

③ 查看是否有相关端口处于异常阻塞状态。如果端口处在异常阻塞状态,说明网络曾经发生过异常。异常阻塞通常与生成树的几种保护机制相关。

以下为根保护机制导致的端口异常阻塞。

命令:*display stp interface GigabitEthernet1/0/1*

```
<H3C>display stp interface GigabitEthernet1/0/1

----[CIST][Port1(GigabitEthernet1/0/1)][DISCARDING]----
 Port Protocol          :enabled
 Port Role              :CISTDesignated Port
Protection Type         :Root
 <H3C>
```

从端口统计上看,端口角色是 Designated Port,但处于 DISCARDING 状态,属于异常阻塞。再看保护类型属于根保护,初步判断是有更高优先级的网桥连接所致。

查看历史告警记录。

命令:<H3C>*display logbuffer reverse*

```
<H3C>display logbuffer   reverse
%Apr 29 10:32:49:322 2000 H3C MSTP/4/MSTP_ROOT_PROTECTION: Instance 0's

ROOT-Protection port GigabitEthernet1/0/2 received superior BPDUs.
%Apr 29 10:32:49:152 2000 H3C MSTP/6/MSTP_DISCARDING: Instance 0's

GigabitEthernet1/0/2 has been set todiscarding state.
%Apr 29 10:32:49:002 2000 H3C MSTP/4/MSTP_ROOT_PROTECTION: Instance 0's

ROOT-Protection port GigabitEthernet1/0/1 received superior BPDUs.
```

从告警记录上看,确实有更高优先级的网桥接入网络导致根保护端口处于 DISCARDING 状态。

以下为环路保护导致的端口异常阻塞。

```
[H3C]display stp interface GigabitEthernet 1/0/1

----[CIST][Port1(GigabitEthernet1/0/1)][DISCARDING]----
 Port Protocol          :enabled
 Port Role              :CISTDesignated Port
Protection Type         :Loop
```

告警信息：

```
<H3C>disp logbuffer  reverse
%Apr 29 11:59:11:132 2000 H3C MSTP/2/BPDURCVDEXPIRY:Instance 0's

Port GigabitEthernet1/0/1 received no message within the rcvdInfoWhile interval. Information of the port wasaged out.
%Apr 29 11:59:11:393 2000 H3C MSTP/2/PDISC:Instance 0's

GigabitEthernet1/0/1 has been set to discarding state!
%Apr 29 11:59:11:563 2000 H3C MSTP/2/LGEXP:Instance0's

LOOP-Protection port GigabitEthernet1/0/1 did not receive message!
```

以下为 BPDU 保护导致的端口异常 Down 状态。

```
[H3C]display stp interface GigabitEthernet 1/0/2

----[CIST][Port2(GigabitEthernet1/0/2)][Down]----
 Port Protocol        :enabled
 Port Role            :CISTDisabled Port
 Port Priority        :128
 Port Edged           :Config=enabled / Active=enabled
 BPDU-Protection      :enabled
```

告警信息：

```
#Apr 29 12:16:27:266 2000 H3C MSTP/1/IVBPDU:hwPortMstiBpduGuarded: BPDU-Protection port 2 received BPDU packet!
%Apr 29 12:16:27:406 2000 H3C MSTP/2/IVBPDU:BPDU-Protection port GigabitEthernet1/0/2 received BPDU packet!
%Apr 29 12:16:27:536 2000 H3C IFNET/4/LINK UPDOWN:
GigabitEthernet1/0/2: link status is Down
```

以下为单端口环路导致的端口异常 DISCARDING 状态。

```
[H3C-GigabitEthernet1/0/2]disp stp int gi 1/0/2

----[CIST][Port2(GigabitEthernet1/0/2)][DISCARDING]----
Port Protocol        :enabled
Port Role            :CISTDesignated Port
Port Edged           :Config=enabled / Active=disabled
Protection Type      :None
```

告警信息：

```
%Apr 29 13:37:54:227 2000 H3C MSTP/2/PDISC:Instance 0's

GigabitEthernet1/0/2 has been set to discarding state!
%Apr 29 13:37:54:368 2000 H3C DRVDBG/4/LOG Info:
Loopback does exist on port GigabitEthernet1/0/2 vlan 1, please check it
```

(7) 检查业务 vlan 是否贯穿全网(仅指该业务 vlan 需要覆盖到的网桥)

查看出现故障的业务 vlan，进行端到端的全部路径的查询。需要确认以下内容。

① 转发路径上每一个端口(网桥互连端口)上正确配置了相应的业务 VLAN。

命令:[H3C]*display interface GigabitEthernet 1/0/1*

```
[H3C]display interface GigabitEthernet1/0/1
 GigabitEthernet1/0/1 current state: Up
PVID: 1
 Mdi type: auto
 Port link-type: trunk
 VLAN passing   : 1(default vlan), 100-110
  VLAN permitted: 1(default vlan), 100-110
  Trunk port encapsulation: IEEE 802.1q
```

② 转发路径上每一个端口(网桥互连端口)上正确学习到了相关 MAC,且多次查看 MAC 是否频繁迁移。

命令:[H3C] *display mac-address xxxx-xxxx-xxxx*

```
[H3C]display mac-address 0000-0000-0021
MAC ADDR          VLAN ID   STATE          PORT INDEX             AGING TIME(s)
0000-0000-0021    100       LEARNED     GigabitEthernet1/0/2        AGING
  ---  1 MAC address(es) found  ---
[H3C]display mac-address 0000-0000-0021
MAC ADDR          VLAN ID   STATE          PORT INDEX             AGING TIME(s)
0000-0000-0021    100       LEARNED     GigabitEthernet1/0/1        AGING

  ---  1 MAC address(es) found  ---
[H3C]
```

如果存在频繁的业务 MAC 飘移,则很可能存在环路问题。需要进行环路的追踪。追踪的原则是判断业务 MAC 正常情况下应该从哪个端口收到,那么从其他的端口收到则可能是环路的端口。通常用 display 看到的端口就是发生环路的端口。

③ 查看转发路径上每一个端口(网桥互连端口)上的流量统计情况,重点关注端口收发报文占用带宽的百分比,组播和广播流量大小。

命令:[H3C]*display interface GigabitEthernet 1/0/1*

```
[H3C]display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
Port priority: 0
 Peak value of input: 108553678 bytes/sec, at 2000-04-29 07:15:01
 Peak value of output: 108553647 bytes/sec, at 2000-04-29 07:15:01
 Last 300 seconds input:   822376 packets/sec 108553662 bytes/sec          100%
 Last 300 seconds output:   822375 packets/sec 108553630 bytes/sec         100%
 Input (total): 453736361 packets, 59892409109 bytes
           0 unicasts, 453604531 broadcasts, 131834 multicasts
 Input (normal):  453736365 packets, 59892409109 bytes
           0 unicasts, 453604531 broadcasts, 131834 multicasts
 Input:   0 input errors, 0 runts, 0 giants, 0 throttles
           0 CRC, 0 frame, 0 overruns, 0 aborts
           0 ignored, 0 parity errors
 Output (total): 453585222 packets, 59873409459 bytes
           0 unicasts, 453579906 broadcasts, 5326 multicasts, 0 pauses
 Output (normal): 453585232 packets, 59873409459 bytes
           0 unicasts, 453579906 broadcasts, 5326 multicasts, 0 pauses
```

```
Output: 0 output errors, 0 underruns, 0 buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, 0 no carrier

[H3C]
```

从端口统计数据看出，如果端口收发数据的百分比超过 90%，并且广播和组播数据占据绝大部分比例时，很可能存在环路。需要追踪此类端口，来判断环路路径。判断方式是在环路路径上的端口收发的广播/组播数据量都很大，未在环路路径上的端口仅发方向的广播/组播流量大。

02

路由技术


杨　勇
表示上一步结果正常
表示上一步结果出现问题
开始
接口打环排查
串口故障排查
线缆及线路排查
接口配置排查
拨打热线
400-810-0504寻求帮助

02 路由技术 > 2.1 接口管理 > 2.1.1 串口故障排查 > 步骤详解

1. 开始

串口问题需关注接口当前状态及线路信号检测，问题多集中在线缆及设备互通性上，定位故障的思路是：首先查看接口状态，检查线缆与线路，最后排查设备双方配置。

2. 流程图相关操作说明

(1) 接口打环排查

通过打环命令来测试接口是否异常，如果打环后接口物理不能 Up 或者接口物理 Up 但是收发包不一致，那么可判断为接口硬件问题，打环前需清空接口计数器统计信息。

命令：*loopback*

清空计数器命令：*reset counters interface interface-type interface-number*

例如：串口视图下使用打环命令，接口会提示 Up，此时查看接口的收发包一致。

```
清空接口计数器统计内容
<H3C>reset counters interface serial 6/0

设备端口打环测试
[H3C-Serial6/0]loopback
%May 15 13:58:42:106 2013 ASBR2 IFNET/3/LINK_UPDOWN: Serial6/0 link status is Up.
[H3C-Serial6/0]display interface serial6/0
Serial6/0 current state: Up
Line protocol current state: Down
Description: Serial6/0 Interface
 Input: 12 packets, 156 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
  Output:12 packets, 156 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
  DCD=Down  DTR=Down  DSR=Down  RTS=Down  CTS=Down
```

(2) 线缆及线路排查

华三通信设备需要配备华三通信的专有接口线缆，线缆分为 DCE 与 DTE 线缆，接口类型随线缆类型确定，与传输及对端设备互联时需保证接口类型匹配。华三通信与运营商对接多使用 DTE 线缆，如图 2-1 所示为华三通信的 DTE 线路。

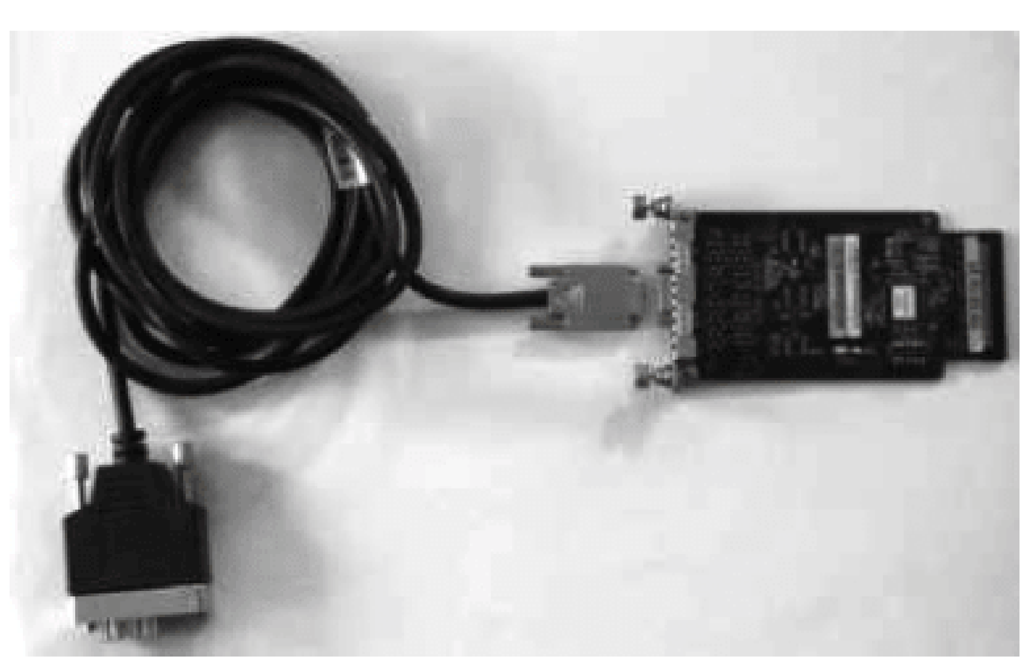


图 2-1 华三通信的 DTE 线路

接口状态显示中包括中 5 种信号检测，具体如表 2-1 所示。

```
[R1]display interface Serial 6/0
Serial6/0 current state: Up
Line protocol current state: Up
Description: Serial6/0 Interface
Output queue : (FIFO queuing : Size/Length/Discards)   0/75/0
Physical layer is synchronous, Virtual baudrate is 64000 bps
Interface is DTE, Cable type is V35, Clock mode is DTECLK1
…
DCD=Up   DTR=Up   DSR=Up   RTS=Up   CTS=Up
```

表 2-1　接口状态

DTR	Data Terminal Ready	DTE 准备好
DSR	Data Set Ready	DCE 准备好
RTS	Request to Send	请求发送
CTS	Clear To Send	准备发送
DCD	Digital Carrier Detector	载波检测

DTR 和 DSR 是第一握手信号，表示本端设备和对端设备的基本状态。RTS、CTS 为第二握手信号，常用于流控使用，同步串口物理 Up 的条件是：接口插的是我司电缆，同时 DSR、DCD 有效。DSR 与 DCD 无法 Up 则可能为运营商侧线路原因导致。

（3）配置排查

查看串口的配置，确定是否正确地配置了串口的相关协商参数，串口无法 Up 一般与接口时钟配置有关，可以尝试修改接口时钟类型与对于接收发送时钟做反转测试。

命令：*display interface serial interface-number*

例如：通过命令查看串口配置，确保两端串口的时钟是否匹配。

```
DTE 侧设备
[DTE]display interface Serial 6/0
Serial6/0 current state: Up
Line protocol current state: Up
…
Interface is DTE, Cable type is V35, Clock mode is DTECLK1

DCE 侧设备
[DCE]display interface Serial 5/0
Serial5/0 current state: Up
Line protocol current state: Up
…
Interface is DCE, Cable type is V35, Clock mode is DCECLK1
```


杨 勇
表示上一步结果正常
表示上一步结果出现问题
E1接口故障排查
开始
接口物理状态
线路排查
接口物理参数排查
相关环境排查
拨打热线
400-810-0504寻求帮助

02 路由技术 > 2.1 接口管理 > 2.1.2 E1 接口故障排查 > 步骤详解

1．开始

常见的 E1 模块问题为接口物理无法 Up，错包较多，其主要原因为接口收到线路告警，或共地不良引起。因此 E1 模块定位故障的思路是：首先检查板卡硬件，然后排查线路，接着排查物理参数，最后检查设备使用环境。

2．流程图相关操作说明

(1) 接口硬件排查

E1 接口的物理故障排查可通过打环进行测试的，观察接口物理是否 Up，并观察逻辑串口上的收发报文是否一致，如果一致可以初步排除板卡硬件问题。需注意的是在查看之前要清空一下接口的收发包，打本地环时，接口不能接线缆，以防线路对环回接口影响。

E1 板卡命令：*loopback local*

E1-F 板卡命令：*fel loopback local*

清空计数器命令：*reset counters interface interface-type interface-number*

例如：通过命令对于 E1 板卡打环，查看接口状态，可检测到环回，且接口 Up、收发包一致，可排除接口卡硬件故障。

```
在本端设备上配置打环
[H3C]controller e11/0
[H3C-E11/0]loopback local
<H3C>reset counters interface serial 1/0:0

在本端设备上查看接口状态
[H3C-E11/0]display interface serial 1/0:0
Serial1/0:0 current state: Up
Line protocol current state: Down
Link layer protocol is PPP, loopback is detected
    Input: 24 packets, 312 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
    Output:24 packets, 312 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
```

(2) 线路排查

查看线缆是否与板卡类型匹配，线缆阻抗与接口阻抗是否匹配，建议使用我司标准线缆。

E1 板卡命令：*display controller E1 interface-number*

E1-F 板卡命令：*display fe1 serial interface-number*

例如：通过命令查看到 E1 1/0 接口需使用 120 欧线缆。

```
[H3C]display controller E1 1/0
E1 1/0/0 current state :Up
```

```
Description : E1 1/0/0 Interface
Basic Configuration:
  Work mode is E1 framed, Cable type is 120 Ohm balanced.
```

通过远端环回测试线路质量，远端环回需要远端设备设置环回，然后在本端设备上查看接口是否能检测到环回，同时查看接口收发包是否一致，查看前需使用命令先清空接口计数器。

E1 板卡命令：*loopback remote*

E1-F 板卡命令：*fel loopback remote*

清空计数器命令：*reset counters interface interface-type interface-number*

例如：在远端设备相对应的 E1 接口下配置远端环回，在本端查看接口状态，可检测到环回，且接口 Up、收发包一致，则可排除线路问题。

```
在远端设备上配置打环
[H3C]controller e11/0
[H3C-E11/0]loopback remote

在本端设备上查看接口状态
<H3C>reset counters interface serial 1/0:0
[H3C-E11/0]display interface serial 1/0:0
Serial1/0:0 current state: Up
Line protocol current state: Down
Link layer protocol is PPP, loopback is detected
    Input: 24 packets, 312 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
    Output:24 packets, 312 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
```

线路排查时，可以要求运营商逐段打环测试，确认线路故障出现节点。

(3) 接口物理参数排查

通过命令确认两端接口下是否有告警，如果有告警，根据告警内容检查端口配置与传输设备及远端设备是否一致。

E1 板卡命令：*display controller E1 interface-number*

E1-F 板卡命令：*display fel serial interface-number*

例如：通过命令查看两端 E1 接口的硬件参数是否一致。是否存在告警，接口是否存在错包，显示信息包括工作模式(成帧或非成帧)、帧格式、CRC 校验方式、编码格式、线路空闲码、帧间填充符、时钟、告警信息、接口错包类型。注意 E1 板卡配置时钟时，两台对接设备的接口时钟为一主一从。

```
[H3C] display controller E1 2/0
E1 2/0 current state: Up
Description : E1 2/0 Interface
Basic Configuration:
Work mode is E1 framed, Cable type is 75 Ohm unbalanced.
```

```
Frame-format is no-crc4.
Line code is hdb3, Source clock is slave.
Idle code is 7e, Itf type is 7e, Itf number is 4.
Loop back is not set.
Alarm State:
Receiver alarm state is None.
Historical Statistics:
Last clearing of counters: Never
Data in current interval (150 seconds elapsed):
0 Loss Frame Alignment Secs, 0 Framing Error Secs,
0 CRC Error Secs, 0 Alarm Indication Secs, 0 Loss-of-signals Secs,
0 Code Violations Secs, 0 Slip Secs, 0 E-Bit error Secs.
```

（4）环境排查

使用 E1 接口对设备环境存在要求，主要为电源环境，要求路由器与传输设备共地。共地不良，对接设备基准电压不同，数据的收发和各种信号的检测不在一个电压平台上，会出现本端发送的数据与对端接收的数据不一致，导致收发出现错包或协议 Up/Down 的现象。


孙培浩
表示上一步结果正常
表示上一步结果出现问题
开始
3G板卡是否识别
3G接入故障排查
USIM卡是否欠费
3G板卡是否支持
确认信号强度
查看3G相关配置
拨打热线
400-810-0504寻求帮助

1．开始

3G 接入问题定位故障的思路是：先确认 3G 板卡是否被识别、USIM 卡是否欠费、信号强度正常，再确认路由器 3G 相关配置。

2．流程图相关操作说明

（1）3G 板卡是否识别

确认 3G 板卡对应的 TTY 接口。

命令：*display user-interface*

例如：通过命令查看，可以看到 Cellular0/0 对应 TTY 13 接口。

```
[H3C] display user-interface
    Idx   Type      Tx/Rx        Modem Privi Auth   Int
+ 0     CON 0      9600         -        3       N      -
  13    TTY 13     9600         -        0       N      Cellular0/0
  177   AUX 0      9600         -        0       P      -
  178   VTY 0                   -        1       A      -
  179   VTY 1                   -        1       A      -
```

在 3G 板卡对应的 TTY 接口下配置呼入呼出权限。

命令：*modem both*

例如：配置 TTY 接口 13 为呼出权限。

```
[H3C] user-interface tty 13
[H3C-ui-tty13] modem both
```

确认路由器是否识别 3G 板卡。

命令：*display cellular interface-number all*

例如：通过命令查看，可以确认路由器已识别 3G 板卡，型号为 E176G。

```
[H3C] display cellular 0/0 all
Modem State:
Hardware Information
------------------------------------------
Model = E176G
Modem Firmware Version = 11.604.09.00.00
Hardware Version= CD25TCPU
International Mobile Subscriber Identity (IMSI) = 460029010431055
International Mobile Equipment Identity (IMEI) = 353871020138548
Factory Serial Number (FSN) =   DK9RAA1871500602
Modem Status = Online
```

（2）3G 板卡是否支持

参考路由器当前版本的版本说明书中 3Gmodem 的型号支持列表内容确认。

（3）USIM 卡是否欠费

可以向运营商确认 USIM 上网卡是否欠费。

(4) 确认信号强度

查看路由器当前所处位置的信号强度,信号强度范围－110dBm～－51dBm,正常使用信号范围:－85dBm～－51dBm,越接近－51dBm信号越好。

命令:*display cellular interface-number all*

例如:通过命令查看,可以看到当前信号强度为－61dBm。

```
[H3C] display cellular 0/0 all
…
Radio Information
--------------------------------
Current Band = ANY
Current RSSI = -61 dBm
```

(5) 查看3G相关配置

查看配置,确保3G modem允许拨入拨出,用户名密码、拨号串、APN等参数正确。

说明:

① TD-SCDMA和WCDMA网络的拨号串是"*99#",CDMA2000网络的拨号串是"#777"。

② 保证配有下一跳为Cellular接口的路由。

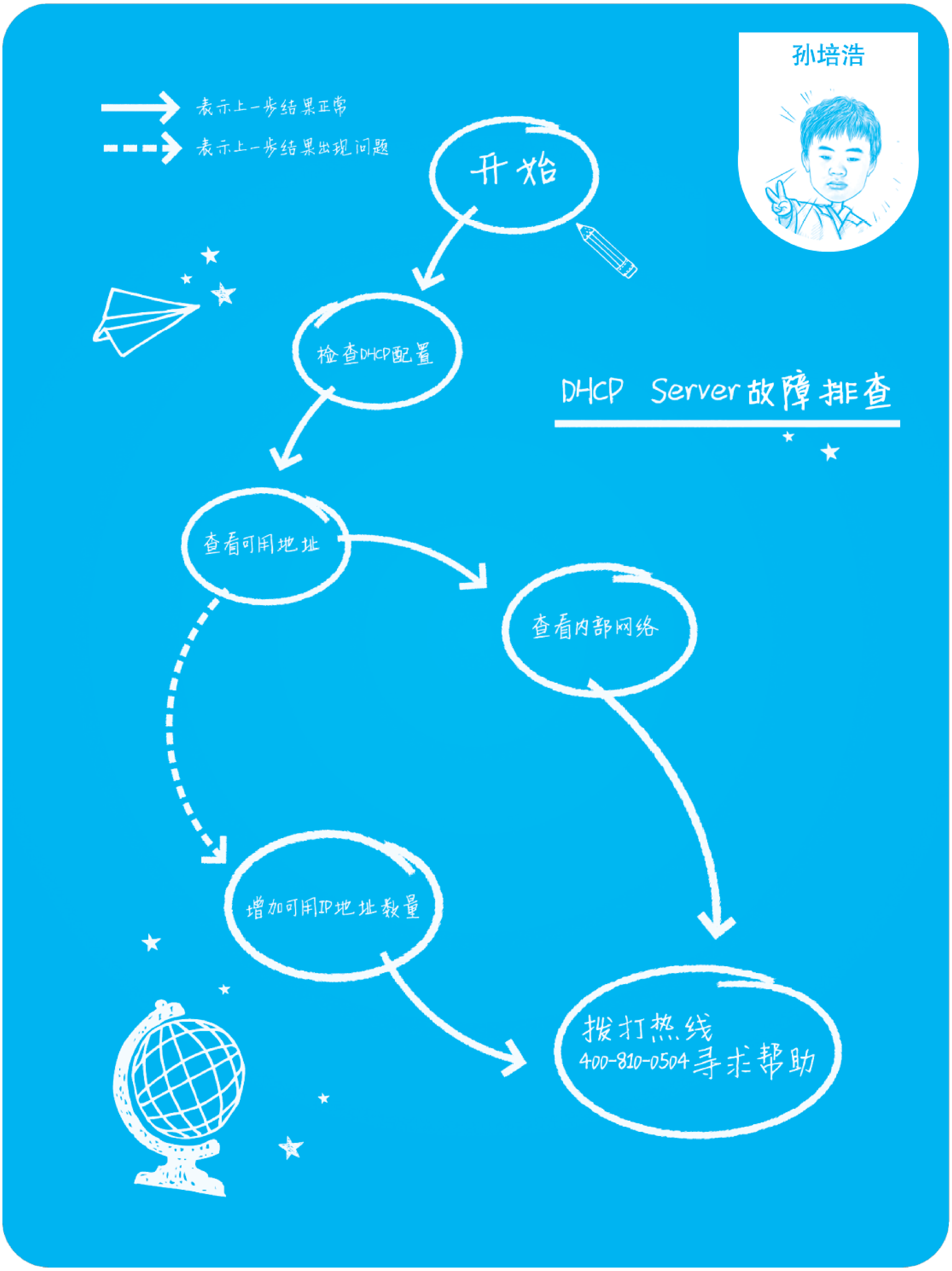
③ 保证APN接入点配置正确。(APN由运营商提供,默认情况下为自动获取的模式,如果在其他配置均正确的情况下3G拨号依然不成功,则需要联系当地运营商确认APN是否与设备当前配置的一致。)

命令:*display current-configuration*

例如:通过命令查看3G配置的用户名为card,密码为card(被加密),拨号串为*99#,user-interface 13已经允许呼入呼出。

```
[H3C]display current-configuration
#
interface Cellular0/0
 async mode protocol
 link-protocol ppp
//由于不确认运营商使用的加密方式,因此建议本端同时配置chap和pap两种方式
 ppp chap user card
 ppp chap password cipher IFB7*Q^N)UCQ=^Q'MAF4<1!!
 ppp pap local-user card password cipher IFB7*Q^N)UCQ=^Q'MAF4<1!!
//配置apn接入点为3gnet,接入点、用户名、密码、验证方式等都需要向运营商确认
 profile create 1 static 3gnet authentication-mode chap user card password card
 ppp ipcp dns request
 ip address ppp-negotiate
 dialer enable-circular
 dialer-group 1
 dialer timer idle 60
 dialer number *99#          //配置拨号串
 nat outbound
#
//配置指向cellular接口的路由
 ip route-static 0.0.0.0 0.0.0.0 Cellular0/0
```

```
#
 dialer-rule 1 ip permit              //定义拨号访问组1允许IP协议的报文通过
#
 user-interface tty 13
   modem both                         //tty接口下要配置modem both
#
```


孙培浩
表示上一步结果正常
表示上一步结果出现问题
DHCP Server故障排查
开始
检查DHCP配置
查看可用地址
查看内部网络
增加可用IP地址数量
拨打热线
400-810-0504寻求帮助

02 路由技术 2.2 IP 业务 2.2.1 DHCP Server 故障排查 步骤详解

1. 开始

DHCP Server 定位故障的思路是：先查 DHCP 的配置，再查看是否存在可用 IP 地址，然后查看内部网络是否正常。

2. 流程图相关操作说明

(1) 检查 DHCP Server 配置

查看当前 DHCP Server 配置，主要包括使能 DHCP，地址池配置。

命令：*display current-configuration*

① 使能 DHCP Server 功能。

[*H3C*]*dhcp enable*

② 配置 DHCP Server 地址池。

[*H3C*] *dhcp server ip-pool X* [*extended*]

例如：通过命令查看，可以确认已使能 DHCP；并配置了 DHCP 地址池 1，可分配的地址段为 172.31.123.10-172.31.123.20，掩码为 255.255.255.0，网关为 172.31.123.1。

```
[H3C]display current-configuration
#
 dhcp enable
#
dhcp server ip-pool 1 extended
 network ip range 172.31.123.10 172.31.123.20
 network mask 255.255.255.0
 gateway-list 172.31.123.1
#
```

(2) 查看可用地址

查看 DHCP Server 地址池是否有可用地址。

命令：*display dhcp server free-ip*

例如：通过命令查看，可以确认 172.31.123.10 至 172.31.123.20 地址还未使用。

```
[H3C] display dhcp server free-ip
IP Range from172.31.123.10     to   172.31.123.20
```

(3) 增加可用 IP 地址数量

如 DHCP Server 地址池无可用地址，则可增加 DHCP 地址池的 IP 地址范围，以此增加该 DHCP 地址池的可用地址数量。

命令：*network ip range min-address max-address*

例如：通过命令查看，可以确认 172.31.123.10 至 172.31.123.20 地址还未使用。

```
<H3C> system-view
[H3C] dhcp server ip-pool 0 extended
[H3C-dhcp-pool-1] network ip range 172.31.123.10 172.31.123.70  //地址池范围由 172.31.123.10
至 172.31.123.20 增大为 172.31.123.10 至 172.31.123.70
```

（4）查看内部网络

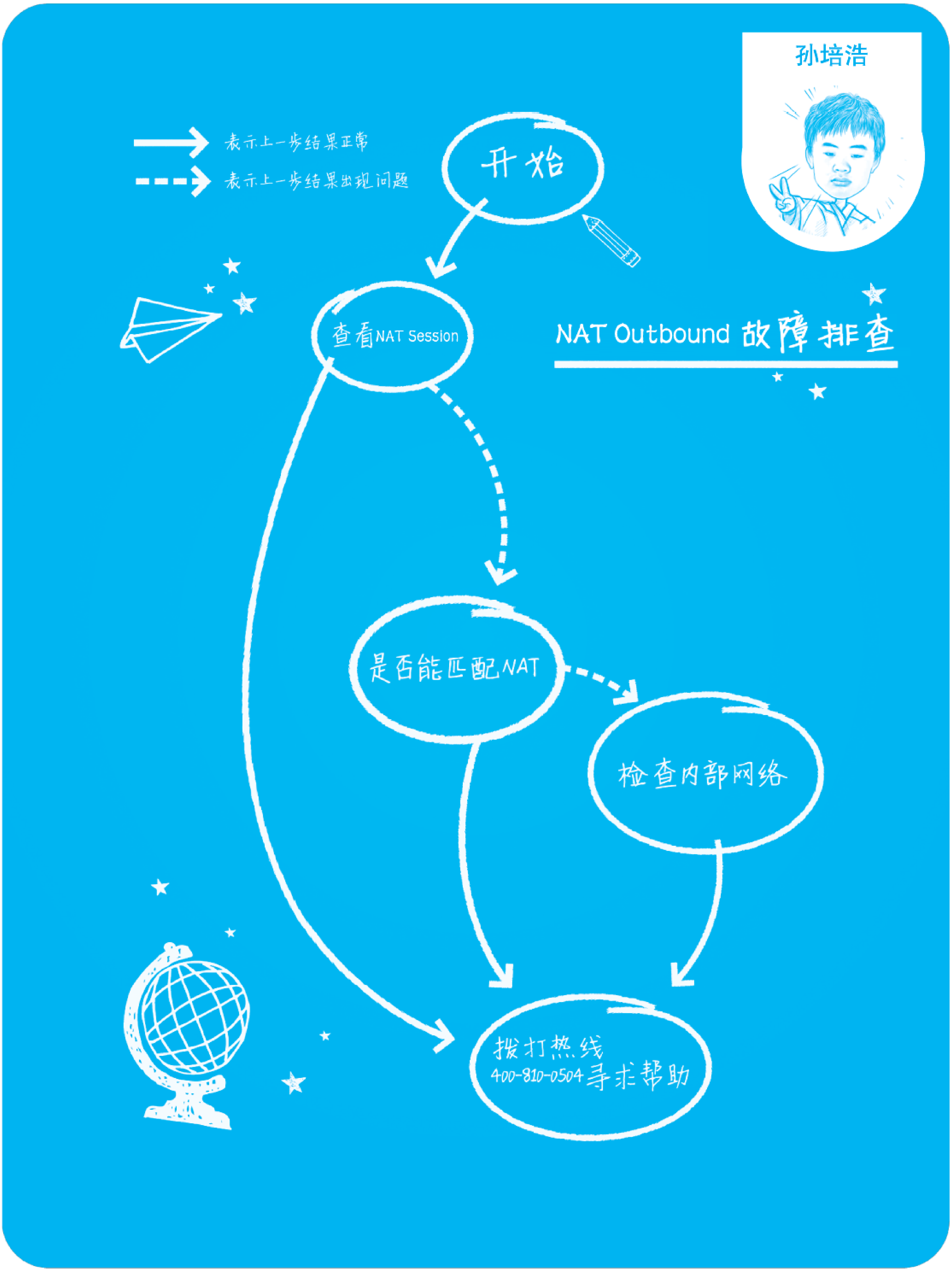
如无 DHCP 中继，则需要排查内部二层网络；如果有 DHCP 中继，则还需要排查中继设备与 DHCP 服务器之间三层网络是否可达。

① 排查二层网络。确认 PC 与 DHCP Server/DHCP Relay 之间是否可达，步骤如下。

PC 配置一个与 DHCP Server/DHCP Relay 同网段的 IP 地址（注意不要和其他地址冲突），然后将 DHCP Server/DHCP Relay 作为网关，使用 PC 来 ping DHCP Server/DHCP Relay，确认是否能够 ping 通。

② 排查三层网络。确认 DHCP Relay 与 DHCP Server 之间是否可达，步骤如下。

分别在 DHCP Relay 上 ping DHCP Server、DHCP Server 上 ping DHCP Relay，看看是否存在 ping 不通，或者单通的现象。


孙培浩
表示上一步结果正常
表示上一步结果出现问题
开始
查看NAT Session
NAT Outbound 故障排查
是否能匹配NAT
检查内部网络
拨打热线
400-810-0504寻求帮助

1. 开始

NAT Outbound 定位故障的思路是：先查 NAT Session，再查看是否能匹配 NAT，然后查看内部网络是否正常。

2. 流程图相关操作说明

(1) 查看 NAT Session

查看 NAT 设备上 NAT Session 是否正常建立。

命令：*display nat session*

例如：通过命令查看，当前 NAT 设备已存在一条 TCP 协议的 NAT Session。

```
[H3C] display nat session
There are currently 1 NAT sessions:
Pro     GlobalAddr:Port        LocalAddr:Port          DestAddr:Port
TCP     10.1.1.1:31391         172.31.123.20:49161     10.1.1.2:5938
        GlobalVPN: ---         LocalVPN: ---
        status: 1              TTL: 00:05:00            Left: 00:04:16
```

(2) 是否能匹配 NAT

首先查看接口下的 NAT 是否有 ACL 过滤，如果有 ACL 过滤，确认报文是否符合 ACL 内容；如果没有 ACL 过滤，则表示所有的流量都能匹配到 NAT。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看，可以确认 interface Ethernet0/0 接口配置的 NAT Outbound 有 ACL 过滤。

```
[H3C] display current-configuration interface Ethernet0/0
#
interface Ethernet0/0
 port link-mode route
 nat outbound 2000
 ip address 10.1.1.1 255.255.255.0
#
return
```

命令：*display acl acl-number*

例如：通过命令查看，可以确认 ACL 2000 规则中只允许 172.31.123.0/24 网段进行 NAT。

```
[H3C]display acl 2000
Basic ACL  2000, named -none-, 2 rules,
ACL's

step is 5
 rule 0 permit source 172.31.123.0 0.0.0.255 (3 times matched)
 rule 1000 deny
```

(3) 检查内部网络

检查访问者设备与 NAT 网关是否路由可达，通常可采用 ping 的方式来判断。


付 睿
开始
NAT-PT故障排查
表示上一步结果正常
表示上一步结果出现问题
检查NAT-PT会话
检查配置信息
修改配置
检查网络状态
拨打热线
00-810-0504寻求帮助

1. 开始

NAT-PT 是在 IPv4 网络完全演变到 IPv6 网络之前，通过映射将 IPv6 和 IPv4 地址进行相互转化从而互通的一种过渡性技术。NAT-PT 机制有静态映射，动态映射和 NAPT-PT。实现过程为：判断是否转换，转换源 IP，转换目的 IP，转发报文并记录映射关系，根据记录的映射关系转发应答报文。NAT-PT 的故障排查思路是：先检查 NAT-PT 会话，再检查配置是否正确，最后检查网络状态。

2. 流程图相关操作说明

(1) 检查 NAT-PT 会话

查看 NAT-PT 设备上的 NAT-PT 会话类型和地址转换情况，判断会话是否正常建立。

命令：*display natpt session all*

例如：通过命令查看，当前 NAT-PT 设备上已经成功建立了一条 NAT-PT 会话。Pro 项 ICMP 代表 NAT-PT 会话的类型为 ICMP。会话的 IPv6 源地址为 2001::0002 被转换为 IPv4 源地址 09.0.0.10。会话的 IPv6 目的地址为 3001::0800:0002，被转换为 IPv4 目的地址 08.0.0.2。此时可以判断源和目的地址都成功转换，会话已经正常建立。

```
[H3C]display natpt session all
 NATPT Session Info:
 No     IPV6Source                  IPV4Source                 Pro
        IPV6Destination             IPV4Destination
1        2001::0002             ^   0 9.0.0.10            ^   0    ICMP
        3001::0800:0002         ^    0 8.0.0.2            ^   0
```

(2) 检查配置信息

分别查看 NAT-PT 设备，IPv4 侧设备和 IPv6 侧设备配置信息。确保 IPv6 侧设备和 NAT-PT 设备使能 IPv6，NAT-PT 设备 NAT-PT 前缀、ACL 和地址映射配置正确，接口下已使能 NAT-PT。

命令：*display current-configuration configuration system*

例如：通过命令查看路由器 IPv6 已使能，NAT-PT 匹配方式为前缀匹配。地址池和前缀已配置，两侧接口下 NAT-PT 已使能。地址映射为 IPv6 侧动态映射，端口不转换。

```
[H3C]display current-configuration configuration system
#
 sysname H3C
#
 domain default enable system
#
 ipv6                                                          //IPV6 已使能
#
 natpt address-group 1 9.0.0.10 9.0.0.19                       //地址池配置
 natpt prefix 3001::                                           //地址前缀配置
 natpt v6bound dynamic prefix 3001:: address-group 1 no-pat    //动态映射配置
#
interface GigabitEthernet0/0
```

```
port link-mode route
 ip address 8.0.0.1 255.255.255.0
 natpt enable                                    //NAT-PT 已使能
#
interface GigabitEthernet0/1
 port link-mode route
 ipv6 address 2001::1/64
 natpt enable                                    //NAT-PT 已使能
#
return
```

例如：通过命令查看路由器 IPv6 已使能，NAT-PT 匹配方式为 ACL 匹配。地址池和 ACL IPv6 已配置，两侧接口下 NAT-PT 已使能。地址映射为 IPv6 侧动态映射，端口默认转换。ACL 匹配所配地址。

```
[H3C]display current-configuration configuration system
#
 sysname H3C
#
 domain default enable system
#
 ipv6                                                    //IPV6 已使能
#
 natpt address-group 1 9.0.0.10 9.0.0.19                 //地址池配置
 natpt prefix 3001::                                     //地址前缀配置
 natpt v6bounddynamic acl6 number 2000 address-group 1   //动态映射配置
#
 acl ipv6 number 2000
 rule 0 permit source 2001::/64                          //ACL IPV6 配置
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 8.0.0.1 255.255.255.0
 natpt enable                                    //NAT-PT 已使能
#
interface GigabitEthernet0/1
 port link-mode route
 ipv6 address 2001::1/64
 natpt enable                                    //NAT-PT 已使能
#
return
```

（3）检查网络状态

根据不同接口类型选配相应的接口线缆，并确保线缆连接正确，端口指示灯正常。通过从 IPv4 侧设备和 IPv6 侧设备 ping NAT-PT 设备，确保网络状态正常可达。从 IPv6 侧 ping 时注意 ping 后要加上 IPv6 字段。

命令：*ping ipv6 ip-address*

例如：通过命令查看 IPv6 侧设备到 NAT-PT 设备网络状态，正常可达。

```
[H3C]ping ipv6 2001::1
  PING 2001::1 : 56   data bytes, press CTRL_C to break
```

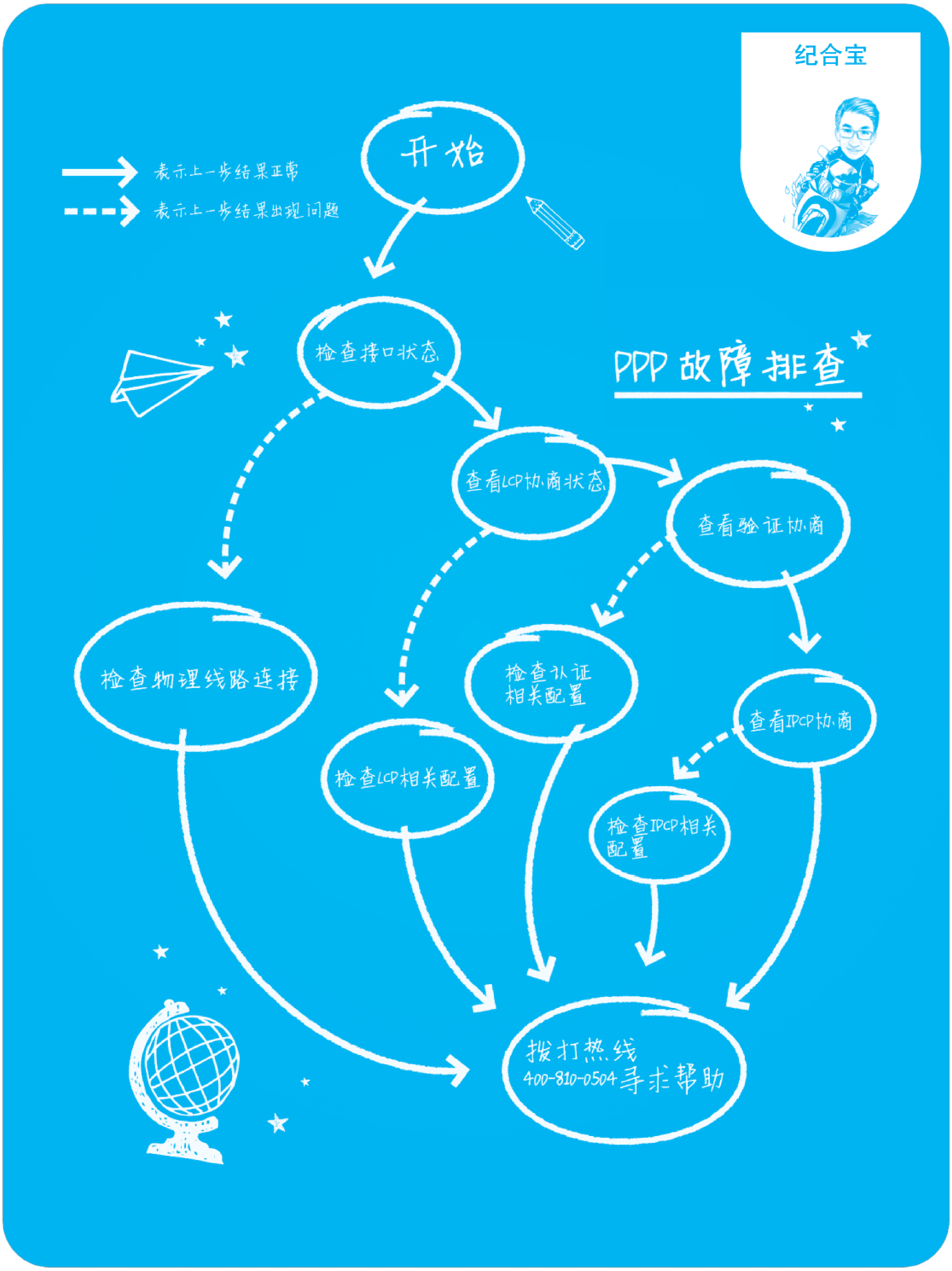
```
    Reply from 2001::1
    bytes=56 Sequence=0 hop limit=64   time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64   time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64   time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=3 hop limit=64   time = 1 ms
    Reply from 2001::1
    bytes=56 Sequence=4 hop limit=64   time = 1 ms
  --- 2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

从 IPv4 侧设备 ping NAT-PT 设备，查看网络状态。

命令：*ping x.x.x.x*

例如：通过命令查看 IPv4 侧设备到 NAT-PT 设备网络状态，正常可达。

```
[H3C]ping 8.0.0.1
  PING 8.0.0.1: 56  data bytes, press CTRL_C to break
    Reply from 8.0.0.1: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 8.0.0.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 8.0.0.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 8.0.0.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 8.0.0.1: bytes=56 Sequence=4 ttl=255 time=1 ms
  --- 8.0.0.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```


纪合宝
表示上一步结果正常
表示上一步结果出现问题
开始
PPP故障排查
检查接口状态
查看LCP协商状态
查看验证协商
检查物理线路连接
检查认证相关配置
查看IPCP协商
检查LCP相关配置
检查IPCP相关配置
拨打热线
400-810-0504寻求帮助

02 路由技术 > 2.3 广域网接入技术 > 2.3.1 PPP 故障排查 > 步骤详解

1. 开始

PPP 协议是提供在点到点链路上传递、封装网络层数据包的一种数据链路层协议，PPP 定义了一整套的协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。PPP 协议定位故障的思路是：从底层查起，先看端口物理层状态，再按照协商顺序依次查看 LCP 协商，验证协商，NCP 协商。

2. 流程图相关操作说明

（1）检查接口状态

分别查看两端设备的接口、协议状态是否 Up。如果接口状态为 Down、LCP 状态为 initial，则说明物理层配置、线缆及设备问题。

命令：*display interface interface-type interface-number*

例如：通过命令查看路由器 Serial 6/1 当前状态 Up，协议 Up。

```
[H3C] display interface Serial 6/1
Serial6/1 current state:Up
Line protocol current state: Up
Description: Serial6/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.0.0.1/24 Primary
Link layer protocol is PPP
LCP opened, IPCP opened
-----------------------------------------------------------
DCD=Up   DTR=Up   DSR=Up   RTS=Up   CTS=Up
```

（2）检查物理连接线路

根据不同接口类型选配相应的接口线缆，并确保线缆连接正确；可通过本地命令做本地环回测试确认板卡是否正常，通过线路上环回测试确认线缆与板卡是否正常，远端设备环回测试确认运营商线路是否正常。具体的打环测试方法请根据接口类型参考相应云图接口故障排查部分。

（3）查看 LCP 状态

若 LCP 未进入 opened 状态，则可考虑为 LCP 协商的问题，首先检查物理接口的报文收发是否正常，如果确认接口的报文收发正常，则排查 LCP 参数协商问题。

命令：*display interface interface-type interface-number*

例如：通过命令查看路由器 Serial 6/1 当前状态 Up，协议 Up，LCP opened 状态，LCP 协商初始状态为 initial，协商过程经过 starting，reqsent，ackrcvd 状态，最终进入 opened 状态。

```
[H3C] display interface Serial 6/1
Serial6/1 current state: Up
Line protocol current state:Up
Description: Serial6/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.0.0.1/24 Primary
```

```
Link layer protocol is PPP
LCPopened， IPCP opened
```

(4) 检查 LCP 配置

LCP 协商无法成功常见配置问题多为设备两端是否验证，MP 捆绑等配置不一致造成，可在两端接口下检查相对应配置是否一致。

命令：*display current-configuration interface interface-type interface-number*

例如：查看互联接口 Serial 6/1 接口下配置，该接口配置 MP 捆绑，则对端设备接口也需要配置 MP 捆绑，双方 MP 配置必须保持一致。

```
[H3C] display current-configuration interface Serial 6/1
#
interface Serial 6/1
 link-protocol ppp
 ppp mp
 ip address 100.1.1.1 255.255.255.0
#
return
```

(5) 查看验证阶段

若 LCP 协议进入 opened 状态，而 IPCP 依然为 initial 状态，或者 LCP 变为 opened 状态后又很快重新开始协商，可考虑为验证的问题；由于此状态为临时状态，不易观察，可通过 debugging ppp all 来观察。如果成功协商了验证，PPP 会打印出 PAP 或 CHAP 验证的报文，如果验证失败，会打印出“PPP authentication failed”信息。

(6) 检查认证相关配置

PPP 认证分为 PAP 与 CHAP 认证，单向与双向，需检查认证方式、用户名与密码是否匹配。

如果接口下配置 ppp authentication-mode 命令，则本端为主验证方，此时可根据 PAP 或 CHAP 验证流程进行验证协商，如果接口下与全局视图都配置 PPP 认证用户名与密码，则协商时首选接口下参数协商。

例如：H3C-A 设备 Serial 6/1 接口与 H3C-B 设备 Serial 5/1 接口互联，H3C-A 设备为主验证方，H3C-B 设备接口下配置发送的验证用户与密码 H3C/H3C。

```
H3C-A 设备配置
#
 local-userH3C
 password simpleH3C
 service-type ppp
#
interface Serial 6/1
 link-protocol ppp
 ppp authentication-mode pap
 ip address 100.1.1.1 255.255.255.0
#

H3C-B 设备配置
#
```

```
interface Serial 5/1
 link-protocol ppp
 ppp pap local-userH3C password simple H3C
 ip address 100.1.1.2 255.255.255.0
#
return
```

(7) 查看 IPCP 状态

若显示 LCP 协议进入 opened 状态，而 IPCP 处于 reqsent 或 stopped，则需要排查 IPCP 参数协商问题。

命令：*display interface interface-type interface-number*

例如：通过命令查看，LCP 状态为 opened 协商通过，IPCP 状态为 opened。

```
[H3C] display interface Serial 6/1
Serial6/1 current state: Up
Line protocol current state: Up
Description: Serial 6/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP opened, IPCP opened
```

(8) 检查 IPCP 配置

IPCP 协商包括：IP 地址、IP 报文压缩协议、DNS 服务器地址等，需检查是否配置正确。

常见配置问题为 IP 地址无法获取，DNS 地址无法获取。

例如：H3C-A 设备接口 Serial 6/1 的 IP 地址需要对端设备分配，H3C-B 设备不允许 H3C-A 设备自行配置接口地址，H3C-B 设备从地址池 pool 1 中为对端分配地址。

```
[H3C-A] display current-configuration interface Serial 6/1
#
interface Serial 6/1
 link-protocol ppp
 ip address ppp-negotiate
#
Return

[H3C-B] display current-configuration interface Serial 5/1
#
interface Serial 5/1
 link-protocol ppp
 ppp ipcp remote-address forced
 remote address pool 1
#
Return
```


纪合宝
表示上一步结果正常
表示上一步结果出现问题
HDLC故障排查
开始
接口物理状态
检查HDLC配置
排查物理线路连接
排查传输线路连通性
拨打热线
400-810-0504寻求帮助

1. 开始

HDLC 是一种面向比特的链路层协议，其定位故障的思路是：从物理层查起，先看端口物理层状态，再查看 HDLC 协商。

2. 流程图相关操作说明

(1) 端口物理状态

分别查看两端路由器的接口状态信息，物理层是否 Up，其中 Down 说明物理层工作异常，应检查两端路由器的物理层配置及设备问题。

命令：*display interface interface-type interface-number*

例如：通过命令查看，路由器物理层 Down，建议排查物理层配置，线缆及设备问题。

```
[H3C] display interface Serial 6/1
Serial6/1 current state:Up
Line protocol current state: Up
Description: Serial6/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.0.0.2/24 Primary
Link layer protocol is HDLC
…
DCD=Up  DTR=Up  DSR=Up  RTS=Up  CTS=Up
```

(2) 检查 HDLC 配置

查看 HDLC 的配置，确定是否正确的配置了 HDLC 相关协商参数，注意两端轮询时间 timer hold 要求配置一致。

命令：*display interface interface-type interface-number*

例如：通过命令查看配置 HDLC 协议，轮询时间为 20 秒。

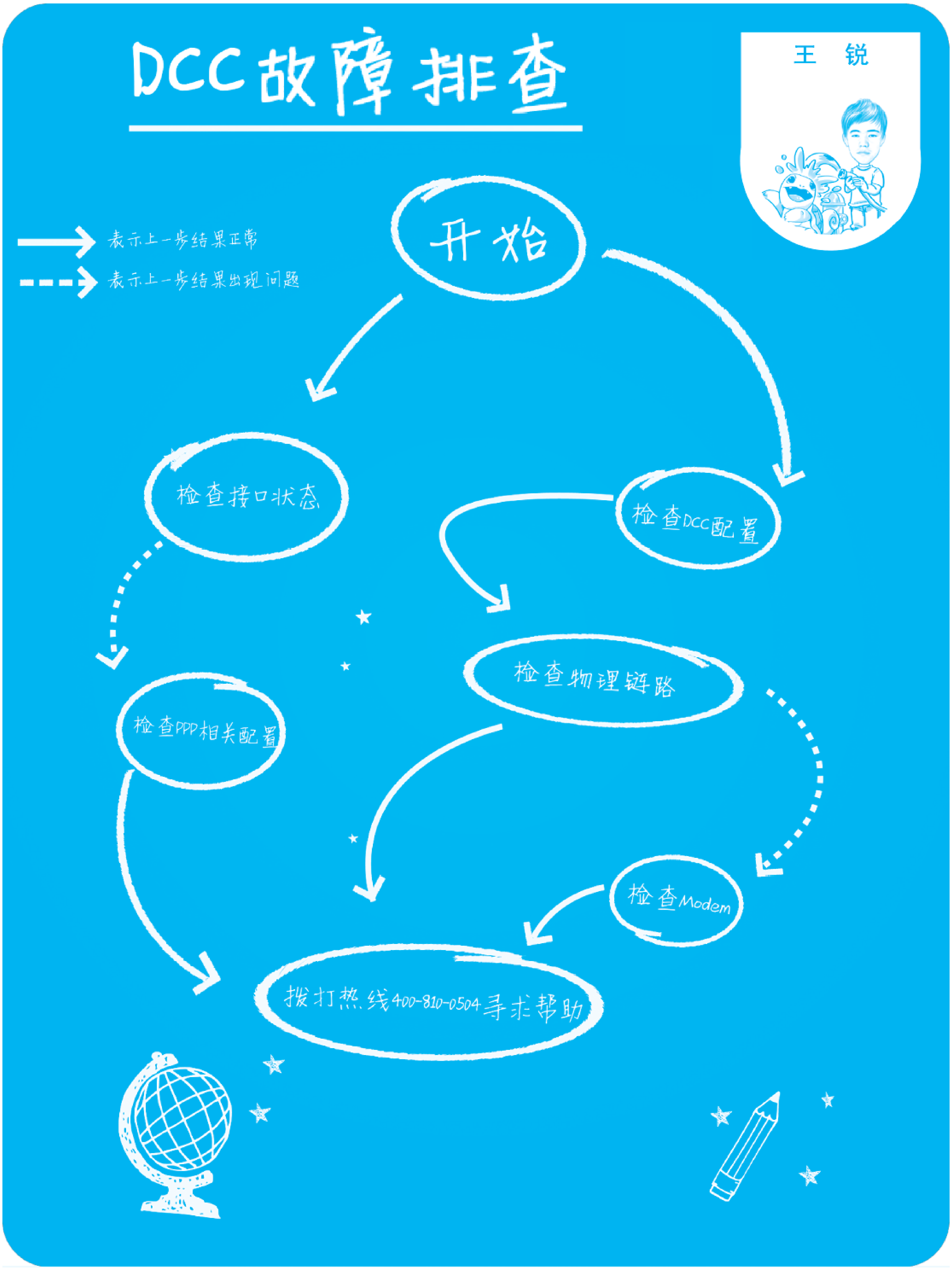
```
[H3C] display interface Serial 6/1
#
interface Serial6/1
 Slink-protocol hdlc
 timer hold 20
 ip address 100.0.0.1 255.255.255.0
#
```

(3) 排查传输线路连通性

可通过远端设备环回测试，确认线路连通性，或者联系运营商设备打环测试，具体的打环测试方法请根据接口类型参考相应云图接口故障排查部分。

(4) 排查物理线路连接

根据不同板卡接口类型选配相应的接口线缆，并确保线缆连接正确；可通过本地环回测试确认板卡硬件是否正常，通过线路环回测试确认线缆与板卡是否正常，远端设备环回测试确认运营商线路是否正常，具体的打环测试方法请根据接口类型参考相应云图接口故障排查部分。


DCC故障排查
王 锐
表示上一步结果正常
表示上一步结果出现问题
开始
检查接口状态
检查DCC配置
检查PPP相关配置
检查物理链路
检查Modem
拨打热线400-810-0504寻求帮助

1. 开始

DCC(Dial Control Center,拨号控制中心)是指路由器之间通过公用交换网进行互联时所采用的路由技术,可以提供按需拨号服务。为了配置 DCC 参数而设置的逻辑接口 Dialer 口,物理接口可以通过绑定到 Dialer 接口而继承配置信息。

DCC 问题定位思路是:先查看接口状态,再查看 DCC 配置,接着查看物理链路,然后检查 Modem,最后查看 PPP 协商过程。

2. 流程图相关操作说明

(1) 检查接口状态

Dialer 口默认协议为 Up,物理状态取决于其对应的物理接口协议层状态。

如果物理接口的物理状态为 Down,则需要排查物理接口及线缆;如果物理接口的物理状态 Up、协议层为 Down,则需要查看物理接口协议层。

命令:*display interface interface-type interface-number*

例如:通过命令查看路由器 Dialer 0 当前状态物理 Up,协议 Up。

```
[H3C]display interface Dialer 0
Dialer0 current state: Up
Line protocol current state: Up (spoofing)
Description: Dialer0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.1.1.1/24 Primary
Link layer protocol is PPP
LCP opened, IPCP opened
```

通过命令查看路由器 Serial 2/1 当前状态物理 Up,协议 Up。

```
[H3C] display interface Serial 2/1
Serial6/1 current state:Up
Line protocol current state: Up
Description: Serial6/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 100.0.0.1/24 Primary
Link layer protocol is PPP
LCP opened, IPCP opened
------------------------------------------------------------
DCD=Up   DTR=Up   DSR=Up   RTS=Up   CTS=Up
```

(2) 检查 DCC 配置

查看 DCC 的配置,包括 DCC 的基本配置、轮询 DCC 的配置、共享 DCC 的配置等。

① 检查 DCC 基本配置。看拨号接口上是否配置链路层协议、接口地址、配置 DCC 拨号控制列表与拨号接口关联以及配置 User-interface 允许 Modem 呼入和呼出。

命令:*display current-configuration*

例如:通过命令查看路由器当前 DCC 相关的配置。

```
[H3C]display current-configuration
#
 dialer-rule 1 ip permit                    //配置拨号控制列表
#
 interface Dialer0
 link-protocol ppp
 ip address 100.1.1.1 255.255.255.0         //配置接口地址
 dialer enable-circular
 dialer-group 1                             //与拨号接口关联
 dialer route ip 100.1.1.2 123
 dialer route ip 100.1.1.3 234
#
 user-interface con 0
 user-interface tty1
 modem both                                 //允许 Modem 呼入与呼出
#
return
```

② 检查轮询 DCC 应用配置。查看拨号接口上是否使能轮询 DCC,并配置呼叫一个或多个对端的拨号串以及轮询 DCC 的关键配置。

命令:*display current-configuration*

例如:通过命令查看路由器当前的轮询 DCC 配置。

```
#
<H3C>system-view
[H3C]dialer-rule 1 ip permit                          //配置拨号访问组 1 以及对应的拨号访问控制条件
#
[H3C]interface dialer 0
[H3C-Dialer0]dialer enable-circular                   //启动轮询 DCC
[H3C-Dialer0]ip address 100.1.1.1 255.255.255.0       //配置 Dialer0 接口 IP 地址
[H3C-Dialer0]dialer-group 1                           //拨号访问组 1 与接口关联
[H3C-Dialer0]dialer route ip 100.1.1.2 8810052
[H3C-Dialer0]dialer route ip 100.1.1.3 8810063        //分别配置到达对端的拨号串
[H3C-Dialer0]quit
#
[H3C]interface serial 2/0
[H3C-Serial2/0]physical-mode async                    //接口工作在异步协议方式
[H3C-Serial2/0]async mode protocol
[H3C-Serial2/0]dialer circular-group 0                //使用的 Dialer Circular Group 组
[H3C-Serial2/0]quit
#
[H3C] interface serial 2/1
[H3C-Serial2/1]physical-mode async                    //接口工作在异步协议方式
[H3C-Serial2/1]async mode protocol
[H3C-Serial2/1]dialer circular-group 0                //使用的 Dialer Circular Group 组
[H3C-Serial2/1]quit
#
[H3C]user-interface tty1
[H3C-ui-tty1]modem both
[H3C-ui-tty1]quit
[H3C]user-interface tty2
[H3C-ui-tty2]modem both                               //配置 User-interface,允许 Modem 呼入和呼出
```

③ 检查共享 DCC 应用配置。分别查看拨号口 Dialer 0、Serial 2/1 是否启动共享 DCC，配置允许接入的对端用户以及配置异步协议方式、配置 PPP 认证信息，配置该接口属于 Dialer bundle1 等各种共享 DCC 关键配置。

命令：*display current-configuration*

例如：通过命令查看路由器当前 Dialer0、Dialer 1 口的共享 DCC 配置。

```
#
<H3C>system-view
[H3C]dialer-rule 1 ip permit                    //配置拨号访问组 1 以及对应的拨号访问控制条件
[H3C]local-user userb
[H3C-luser-userb]password simple userb
[H3C-luser-userb]service-type ppp
[H3C-luser-userb]quit                           //配置 PPP 验证的本地用户 userb
[H3C]local-user userc
[H3C-luser-userc]password simple userc
[H3C-luser-userc]service-type ppp
[H3C-luser-userc]quit                           //配置 PPP 验证的本地用户 userc
#
[H3C]interface dialer 0
[H3C-Dialer0]ip address 100.1.1.1 255.255.255.0   //配置 Dialer0 接口的 IP 地址
[H3C-Dialer0]dialer user userb                    //配置允许拨入的对端用户名
[H3C-Dialer0]dialer bundle 1                      //启动共享 DCC
#
[H3C-Dialer0]dialer-group 1
[H3C-Dialer0]ppp authentication-mode pap          //配置 PPP 认证信息
[H3C-Dialer0]ppp pap local-user usera password simple usera
[H3C-Dialer0]dialer number 8810052                //配置到达对端的拨号串
[H3C-Dialer0]quit
#
[H3C]interface dialer 1
[H3C-Dialer1]ip address 122.1.1.1 255.255.255.0   //配置 Dialer1 接口的 IP 地址
[H3C-Dialer1]dialer user userc                    //配置允许拨入的对端用户名
[H3C-Dialer1]dialer bundle 2                      //启动共享 DCC
#
[H3C-Dialer1]dialer-group 1
[H3C-Dialer1]ppp authentication-mode pap          //配置 PPP 认证信息
[H3C-Dialer1]ppp pap local-user usera password simple usera
[H3C-Dialer1]dialer number 8810063                //配置到达对端的拨号串
[H3C-Dialer1]quit
```

通过命令查看路由器物理接口 Serial 2/0、Serial 2/1 当前的共享 DCC 配置。

```
#
[H3C]interface serial 2/0
[H3C-Serial2/0]physical-mode async              //配置接口工作在异步协议方式
[H3C-Serial2/0]async mode protocol
[H3C-Serial2/0]dialer bundle-member 1           //配置该接口属于 Dialer bundle1
[H3C-Serial2/0]dialer bundle-member 2           //配置该接口属于 Dialer bundle2
[H3C-Serial2/0]link-protocol ppp
[H3C-Serial2/0]ppp authentication-mode pap      //配置 PPP 认证信息
[H3C-Serial2/0]ppp pap local-user usera password simple usera
[H3C-Serial2/0]quit
```

```
#
[H3C]interface serial 2/1
[H3C-Serial2/1]physical-mode async                //配置接口工作在异步协议方式
[H3C-Serial2/1]async mode protocol
[H3C-Serial2/1]dialer bundle-member 1             //配置该接口属于 Dialer bundle1
[H3C-Serial2/1]dialer bundle-member 2             //配置该接口属于 Dialer bundle2
[H3C-Serial2/1]link-protocol ppp
[H3C-Serial2/1]ppp authentication-mode pap        //配置 PPP 认证信息
[H3C-Serial2/1]ppp pap local-user usera password simple usera
[H3C-Serial2/1]quit
#
[H3C]user-interface tty1
[H3C-ui-tty1]modem both                           //允许 Modem 呼入和呼出
[H3C-ui-tty1]quit
[H3C]user-interface tty2
[H3C-ui-tty2]modem both
```

(3) 检查物理链路

根据不同接口类型选配相应的接口线缆，并确保线缆连接正确；可通过本地命令做本地环回测试确认板卡是否正常，通过线路上环回测试确认线缆与板卡是否正常，远端设备环回测试确认运营商线路是否正常。具体的打环测试方法请根据接口类型参考相应云图接口故障排查部分。

(4) 检查 Modem

在拨号端用电话座机替代设备，拨打对端号码，查看是否能听到清晰的 Modem 音。

(5) 检查 PPP 协议

PPP 协议排查具体方法请参考云图中 PPP 排错章节。


陈丹威
开始
FR 故障排查
表示上一步结果正常
表示上一步结果出现问题
检查接口物理状态
检查协议状态
检查接口配置
检查MAP配置
拨打热线
00-810-0504寻求帮助

02 路由技术 ＞ 2.3 广域网接入技术 ＞ 2.3.4 FR 故障排查 ＞ 步骤详解

1. 开始

帧中继(Frame-Relay)协议是链路层协议,它是在 X. 25 技术基础之上发展起来的一种快速分组交换技术。目前帧中继使用最多的方式是永久虚电路方式,即手工配置产生的虚电路方式。帧中继协议定位故障的思路是:从底层开始,先看端口物理状态、再看协议状态,最后检查相关路由协议配置。

2. 流程图相关操作说明

(1) 检查接口物理状态

分别查看两端设备的接口物理状态是否 Up。

如果接口的物理 Down,则需要检查板卡与连接线缆是否正常,交叉测试确定故障原因,具体参考其他云图。

命令: *display interface interface-type interface-number*

例如:通过命令查看路由器 Serial 1/1 当前状态 Up,协议 Down。

```
[H3C]display interface Serial1/1
Serial6/0 current state: Up
Line protocol current state: Down
Description: Serial1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24 Primary
Link layer protocol is FR IETF
  LMI DLCI is 0, LMI type is ANSI, frame relay DCE
  LMI status enquiry received 214, LMI status sent 214
  LMI status enquiry timeout 0, LMI message discarded 4
…
```

(2) 检查协议状态

分别查看两端设备接口的协议状态是否 Up。

两台路由器背靠背连接,在串口上封装帧中继,若接口物理层为 Up、协议层 Down,则可能是由于两端均为 DCE 或 DTE、两端接口的 LMI 类型不一致导致。

若背靠背连接的串口上,接口物理层和协议层均为 Up 状态,却无法 ping 通,则可能是由于 MAP 配置有误导致。

命令: *display interface interface-type interface-number*

例如:通过命令查看路由器 Serial 1/1 当前状态 Up,协议 Up。

```
[H3C]display interface Serial1/1
Serial6/0 current state: Up
Line protocol current state:Up
Description: Serial1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24 Primary
Link layer protocol is FR IETF
  LMI DLCI is 0,LMI type is ANSI, frame relay DCE
```

```
    LMI status enquiry received 214, LMI status sent 214
    LMI status enquiry timeout 0, LMI message discarded 4
...
```

(3) 检查接口配置

H3C 路由器封装 FR 时的默认 LMI 类型是 Q933a。当 DCE 端的 LMI 类型为 Q933a,而 DTE 端配置的 LMI 类型为 ANSI 时,会因为两端的 LMI 类型不一致,而造成链路层协议无法 Up。此时只需将两端的 LMI 类型保持一致即可:配置两端 LMI 类型均为 ANSI,或删除掉对 DTE 侧 LMI 的配置,默认情况下均为 Q933a。

命令:*display interface interface-type interface-number*

例如:通过命令查看路由器 Serial 1/1 当前状态 Up,协议 Up。

```
[H3C]display interface Serial1/1
Serial6/0 current state: Up
Line protocol current state:Up
Description: Serial1/1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24 Primary
Link layer protocol is FR IETF
    LMI DLCI is 0, LMI type is ANSI, frame relay DCE
    LMI status enquiry received 214, LMI status sent 214
    LMI status enquiry timeout 0, LMI message discarded 4
...
```

(4) 检查 MAP 相关配置

直连设备的串口配置帧中继后,分配了同一网段的 IP 地址,接口物理状态和协议状态都 Up 了,却无法 ping 通。这可能是由于缺少了 MAP 配置导致的。

配置了 FR 的接口只要 LMI 类型与对端一致,则协议就会 Up,不管是否配置了 IP 地址,也不管是否有到对端的 MAP。而在帧中继网络中要想互通,除了接口协议要 Up,还要有相应的 MAP,无论是静态还是动态 MAP。

命令:*display current-configuration interface interface-type interface-number*

例如:查看互联接口两端接口的配置,若均没有到对端的 MAP,需要配置。一端配置 MAP 后,另一端默认开启了 InARP,可以动态学习,不用手动配置。

```
[H3C]display current-configuration interfaceSerial 1/1
#
interface Serial1/1
 link-protocol fr
 fr interface-type dce
 fr map ip 1.1.1.2 100
 ip address 1.1.1.1 255.255.255.0
#
return
```


孙培浩
表示上一步结果正常
表示上一步结果出现问题
开始
检查两端GRE配置
GRE VPN 故障排查
查看接口状态
检查私网路由配置
检查两端之间的网络
拨打热线
400-810-0504寻求帮助

02 路由技术 > 2.4 VPN > 2.4.1 GRE VPN 故障排查 > 步骤详解

1. 开始

GRE VPN 定位故障的思路是：先查配置，再查接口状态，然后查两端之间的网络，最后查私网路由。

2. 流程图相关操作说明

(1) 检查两端 GRE 配置

分别查看两端 GRE 配置是否正确。

命令：*display current-configuration interface Tunnel number*

例如：通过命令查看，可以确认两端 GRE 当前配置。

```
本端：
[H3C-A] display current-configuration interface Tunnel 1
#
interface Tunnel1
 ip address 10.0.0.1 255.255.255.252
 source 192.168.1.1
 destination 192.168.2.1
#
return
本端：
[H3C-B] display current-configuration interface Tunnel 1
#
interface Tunnel1
 ip address 10.0.0.2 255.255.255.252
 source 192.168.2.1
 destination 192.168.1.1
#
return
```

(2) 查看接口状态

分别查看两端 tunnel 接口协议是否 Up。

命令：*display interface Tunnel number*

例如：通过命令查看，可以确认 tunnel 接口的协议是 Up 的。

```
本端：
[H3C-A] display interface Tunnel 1
Tunnel1 current state: Up
Line protocol current state: Up
Description: Tunnel1 Interface
The Maximum Transmit Unit is 1476
Internet Address is10.0.0.1/30 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source192.168.1.1 (GigabitEthernet0/1), destination 192.168.2.1
Tunnel bandwidth 64 (kbps)
Tunnel keepalive disabled
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
```

```
对端：
[H3C-B] display interface Tunnel 1
Tunnel1 current state: Up
Line protocol current state: Up
Description: Tunnel1 Interface
The Maximum Transmit Unit is 1476
Internet Address is10.0.0.2/30 Primary
Encapsulation is TUNNEL, service-loopback-group ID not set.
Tunnel source192.168.2.1 (GigabitEthernet0/1), destination 192.168.1.1
Tunnel bandwidth 64 (kbps)
Tunnel keepalive disabled
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
```

（3）检查两端之间的网络

Tunnel 口状态为 Down，需要分为以下两种情况排查。

① Tunnel 口下没有配置 Keepalive，此时需要查看是否存在到达 Destination IP 的公网路由。

命令：*display ip routing-table*

例如：通过查看路由表，可以确认到 Destination IP 地址为 192.168.2.1 的路由存在。

```
[H3C-A] display ip routing-table
Routing Tables: Public
        Destinations : 2          Routes : 2
Destination/Mask    Proto   Pre  Cost       NextHop         Interface
192.168.2.0/24       Direct 0     0          192.168.1.2     GE0/1
192.168.100.0/24     Static 60   0          10.0.0.1        Tun1
```

② Tunnel 口下配置 Keepalive，此时不仅需要查看是否存在到达 Destination IP 的公网路由，还需要确认 Destination IP 是否可达。

命令：*ping -a x.x.x.x x.x.x.x*

例如：通过命令可以看到，在 H3C-A 上指定源 192.168.1.1 ping H3C-B 的 192.168.2.1 可以 ping 通。

```
[H3C-A] ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 192.168.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

（4）检查私网路由

查看到远端私网的路由是否指向了本端的 Tunnel 接口。

命令：*display ip routing-table*

例如：通过查看路由表，可以确认到远端私网 192.168.100.0/24 网段的路由指向了 Tunnel 1 接口。

```
[H3C-A] display ip routing-table
Routing Tables: Public
         Destinations : 2          Routes : 2
Destination/Mask      Proto   Pre  Cost       NextHop         Interface
192.168.2.0/24        Direct  0    0          192.168.1.2     GE0/1
192.168.100.0/24      Static  60   0          10.0.0.1        Tun1
```


孙培浩
L2TP VPN 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查LAC与LNS是否路由可达
查看L2TP隧道
查看L2TP会话
检查LAC,LNS上是否使能L2TP
检查用户认证相关设备的配置
检查LAC,LNS两侧L2TP配置
拨打热线400-810-0504寻求帮助

02 路由技术 > 2.4 VPN > 2.4.2 L2TP VPN 故障排查 > 步骤详解

1. 开始

L2TP VPN 定位故障的思路是：先确认 LAC、LNS 的连通性，再查看 L2TP 隧道是否建立，最后查用户的认证。

2. 流程图相关操作说明

(1) 检查 LAC 与 LNS 是否路由可达

① 分别查看 LAC、LNS 路由器的路由表中是否存在到达对端的路由，并确认是否路由可达。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看，可以确认 LAC 路由器上存在到达对端 LNS 的路由 0.0.0.0/0，下一跳是 10.0.0.1。

```
[LAC]display ip routing-table 0.0.0.0
Routing Tables: Public
        Destinations : 2          Routes : 2
Destination/Mask     Proto   Pre  Cost          NextHop        Interface
0.0.0.0/0            Static  60   0             10.0.0.1       Eth0/0
```

② 检查 LAC 和 LNS 之间是否路由可达。

命令：*ping x.x.x.x*

例如：通过命令可以看到，LAC 到达 LNS 之间路由可达。

```
[LAC]ping 10.0.1.2
  PING 10.0.1.2: 56 data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=0 ttl=255 time=32 ms
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=23 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=23 ms
  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 23/26/32 ms
```

(2) 查看 L2TP 隧道是否建立

查看 LAC、LNS 之间的 L2TP 隧道是否正常建立。

命令：*display l2tp tunnel*

例如：通过命令查看，可以确认 L2TP 隧道已成功建立。

```
[LAC] display l2tp tunnel
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress     Port   Sessions  RemoteName
 1        1         10.0.1.2          1701   1         lns
```

(3) 检查 LAC、LNS 上是否使能 L2TP

确认 LAC、LNS 路由器配置中是否存在 l2tp enable 命令。

命令：*display current-configuration | include l2tp enable*

例如：通过命令查看，可以确认 LAC 路由器上存在 l2tp enable 命令，使能了 L2TP 功能。

```
[LAC] display current-configuration | include l2tp enable
 l2tp enable

[LNS] display current-configuration | include l2tp enable
 l2tp enable
```

(4) 检查 LAC、LNS 两侧 L2TP 配置

确认 LAC、LNS 路由器 L2TP 配置中隧道验证、隧道名称参数是否对应。

确认 LAC 路由器配置的发起 L2TP 连接请求参数是否正确。

确认 LNS 路由器配置的接收 L2TP 连接请求参数是否正确。

```
[LAC] display current-configuration
#
 l2tp enable
#
domain system
 authentication ppp local
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
local-user user1
 password cipher $c$3$W1YxAfpVMZsGDe1UxUGBJEPB20O6RG+G
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 start l2tp ip 10.0.1.2 domain system
#
interface Virtual-Template1
 ppp authentication-mode chap domain system
 ip address 1.1.1.1 255.255.255.0
#
interface Ethernet5/0
 port link-mode route
 pppoe-server bind Virtual-Template 1
#

[LNS] display current-configuration
#
 l2tp enable
#
domain system
 authentication ppp local
 access-limit disable
 state active
```

```
  idle-cut disable
  self-service-url disable
  ip pool 1 192.168.0.2 192.168.0.10
 #
local-user user1
  password cipher $c$3$nH3DI7gxrRRbVjEB+lUxm5j+2LFtow==
  service-type ppp
 #
l2tp-group 1
  undo tunnel authentication
  allow l2tp virtual-template 1
 #
interface Virtual-Template1
  ppp authentication-mode chap domain system
  remote address pool 1
  ip address 192.168.0.1 255.255.255.0
 #
```

（5）查看 L2TP 会话

查看 LNS 上是否存在用户 L2TP 会话。

命令：*display l2tp session*

例如：通过命令查看，可以确认本端已存在一个 L2TP 会话。

```
[LNS] display l2tp session
  Total session = 1
  LocalSID RemoteSID LocalTID
    17922      12990       1
```

（6）检查用户认证相关设备的配置

确认 LNS 路由器配置的用户认证方式是本地认证，还是远端 AAA 认证。

如果是本地认证，则确认输入的用户名密码是否与 LNS 路由器上配置的一致。

如果是远端 AAA 认证，则确认 AAA 配置是否正确、AAA 服务器上配置是否正确。

命令：*debugging ppp all*

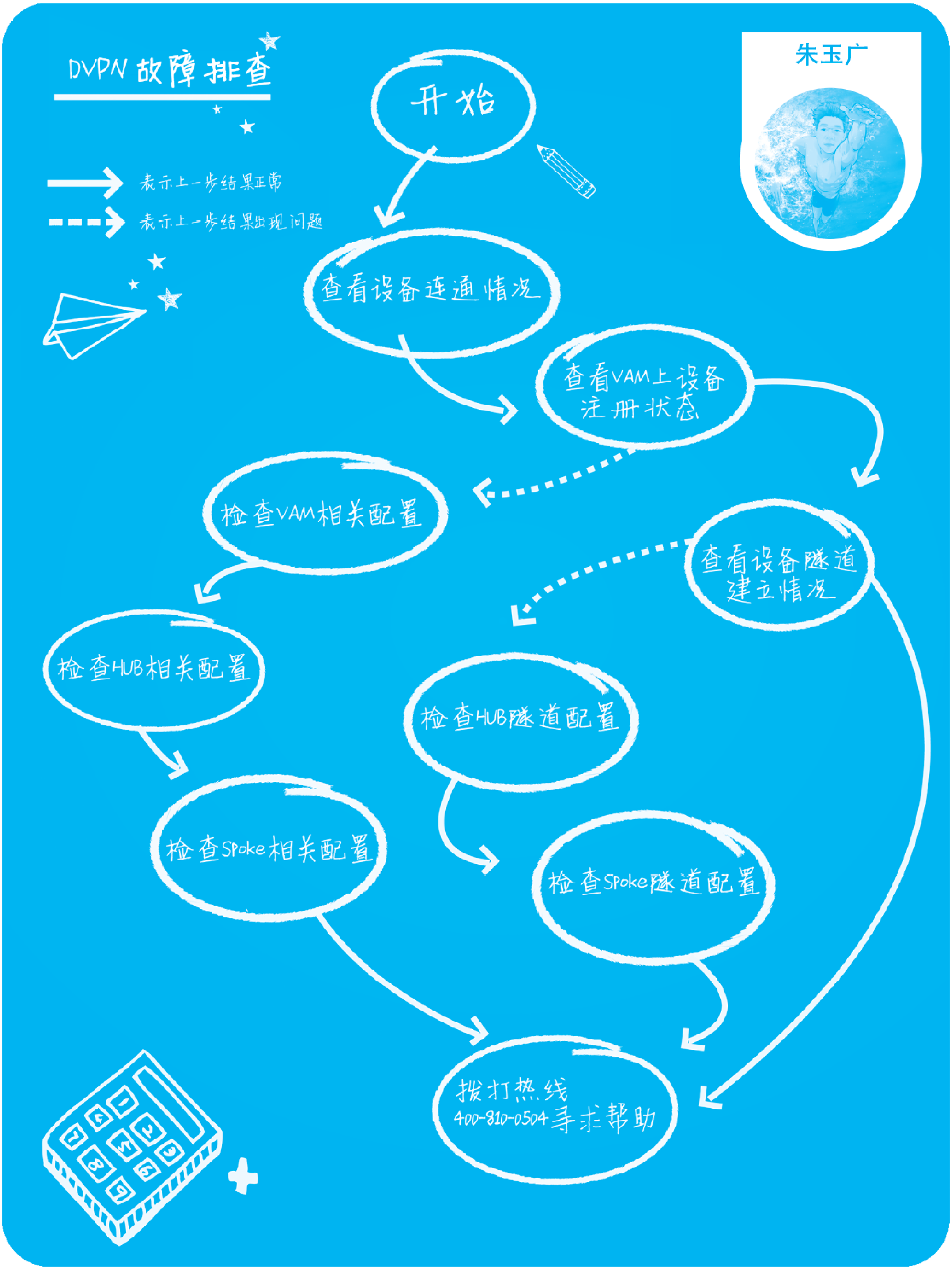
terminal debugging

terminal monitor

例如：通过命令可以查看到由于 AAA 服务器上配置的密码与用户拨入密码不符，验证失败的信息。

```
<LNS>debugging ppp all
<LNS>terminal debugging
<LNS>terminal monitor
//PPP 向 AAA 服务器发送认证信息:
 * Jul 1 14:09:14:212 2013 rta PPP/7/debug2:
   PPP Event:
       Virtual-Template1:0 : PPP send AAA Prim: ulPrimID = 00000002,ulUserID = 0xffffffff
       Detail: ausVlanTag[0] = 65535, ausVlanTag[1] = 65535,
               ulServiceType = 0x6005, ulUserType = 0x10,
               szCallingNumber =
```

```
*Jul 1 14:09:14:215 2013 rta PPP/7/debug2:
//PPP 侧从 AAA 侧收到认证失败的信息
 PPP Event:
     Virtual-Template1:0 : Receive AAA Reject Message, Authen failed!!
*Jul 1 14:09:14:215 2013 rta PPP/7/debug2:
 PPP Event:
     Virtual-Template1:0 CHAP AAA Result Event
     state WaitingAAA
//PPP 报错,chap 验证失败
*Jul 1 14:09:14:215 2013 rta PPP/7/debug2:
 PPP Error:
     Virtual-Template1:0 CHAP : Server authentication failed No. 1 !
*Jul 1 14:09:14:215 2013 rta PPP/7/debug2:
 PPP State Change:
     Virtual-Template1:0 CHAP : WaitingAAA --> ServerFailed
//PPP 侧告警,验证失败,原因为用户的密码非法
*Jul 1 14:09:14:216 2013 rta PPP/7/debug2:
 PPP Packet:
     Virtual-Template1:0 Output CHAP(c223) Pkt, Len 33
     State ServerFailed, code FAILURE(04), id 1, len 29
     Message: Illegal user or password.
```


DVPN 故障排查
表示上一步结果正常
表示上一步结果出现问题
朱玉广
开始
查看设备连通情况
查看VAM上设备注册状态
检查VAM相关配置
查看设备隧道建立情况
检查HUB相关配置
检查HUB隧道配置
检查Spoke相关配置
检查Spoke隧道配置
拨打热线
400-810-0504寻求帮助

02 路由技术 > 2.4 VPN > 2.4.3 DVPN 故障排查 > 步骤详解

1. 开始

DVPN 采用 Client/Server 模式，工作在 TCP/IP 协议栈的应用层。DVPN 支持 UDP 和 GRE 两种隧道类型，按照工作方式的不同，可将一个 VPN 域中的设备划分为一个 Server 和多个 Client，Server 的公网地址为静态地址，Client 的公网地址既可以静态配置也可以动态获取，而 Client 的私网地址则需要按照规划静态分配。在同一个 VPN 域内，要求所有节点的私网地址在同一个网段内。DVPN 故障的定位思路是：首先检查设备间的连通情况，然后检查 VAM Server 上的设备注册情况，最后检查 Hub、Spoke 间的设备间的隧道建立、配置情况。

2. 流程图相关操作说明

(1) 检查设备连通情况

分别查看不同设备间的网络连通情况，如果设备之间不能够 ping 通，则怀疑设备间物理连线或者接口配置有问题。

命令：*ping destination-ip-address*

例如：通过命令检查设备间的连接情况。

```
[H3C] ping 192.168.1.4
  PING 192.168.1.4: 56   data bytes, press CTRL_C to break
    Reply from 192.168.1.4: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.168.1.4: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 192.168.1.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

(2) 检查 VAM Sever 上设备注册状态

若 Hub 和 Spoke 设备中某一设备没有注册到 VAM Sever，则说明该设备与 VAM Server 之间的链路存在问题，下一步则要检查该设备与 VAM Server 上的配置参数是否一致。

命令：*display vam server address-map all*

例如：通过命令查看 VAM Server 上设备的注册状态，如果其中有一台 Spoke 或者 Hub 设备没有注册到 VAM Server 上，该设备将不会显示出来。所有的 Hub 和 Spoke 设备均已经注册到了 VAM Server。

```
<vamserver>display vam server address-map all
  VPN name:   1
  Total address-map number:   4
```

```
Private-ip      Public-ip        Type          Holding time

 10.0.1.1       192.168.1.1      Hub           0H 41M 19S
 10.0.1.2       192.168.1.2      Hub           0H 38M 57S
 10.0.1.3       192.168.1.3      Spoke         0H 40M 46S
 10.0.1.4       192.168.1.4      Spoke         0H 40M 25S

 VPN name:  2
 Total address-map number:  3

 Private-ip     Public-ip        Type          Holding time

 10.0.2.1       192.168.1.1      Hub           0H 41M 19S
 10.0.2.2       192.168.1.2      Hub           0H 38M 57S
 10.0.2.4       192.168.1.4      Spoke         0H 40M 25S
```

(3) 检查 VAM Sever 设备配置情况

在 VAM Sever 需要检查监听 IP 地址、预共享密钥、本地用户名及密码，与 Hub 和 Spoke 设备上的设置是否一致，如果不一致将会导致 Hub 和 Spoke 设备无法注册到 VAM Sever 上。

```
#
 vam server ip 192.168.1.22          //指定 VAM Server 上的监听 IP 地址
#
 vam server vpn 1                    //创建 VPN，域 ID 为 1
 server enable
 pre-shared-key simple 123           //设置预共享密钥
 hub private-ip 10.0.1.1             //指定 VPN 1 的两个 Hub 地址
 hub private-ip 10.0.1.2
#
 local-user dvpn1hub1                //创建本地 Hub 用户
 password simple dvpn1hub1           //设置用户密码
 authorization-attribute level 3
 service-type dvpn                   //服务类型设置为 DVPN
 local-user dvpn1spoke1              //创建本地 Spoke 用户
 passwordsimple dvpn1spoke1          //设置用户密码
 authorization-attribute level 3
 service-type dvpn                   //服务类型设置为 DVPN
```

(4) 检查 Hub 设备相关配置

检查 VAM Client 是否启动，Hub 设备上的相关配置参数要与服务器上的相关参数是否一致，必须保持一致，才能够使得该设备正确注册到 VAM Server 上。

```
#
vam client name dvpn1hub1
 client enable
 server primary ip-address 192.168.1.22            //对应于 VAM Server 地址
 user dvpn1hub1 passwordsimple dvpn1hub1           //对应于 VAM Server 上用户名和密码
 pre-shared-key ciphersimple 123                   //设置预共享密钥
#
```

(5) 检查 Spoke 设备相关配置

检查 VAM Client 是否启动，Spoke 设备上的相关配置参数要与服务器上的相关参数必须保持一致，才能够使得该设备正确注册到 VAM Server 上。

```
#
vam client name dvpn1spoke1
 client enable
 server primary ip-address 192.168.1.22              //对应于 VAM Server 地址
 user dvpn1spoke1 password simple dvpn1spoke1        //对应于 VAM Server 上用户名密码
 pre-shared-key ciphersimple 123                     //设置预共享密钥
#
```

（6）查看设备隧道建立情况

Hub 设备和 Spoke 设备之间，Hub 设备和 Hub 设备之间常见的问题主要是链路问题，可在 Hub 设备上检查 Hub 与其他设备之间建立起的隧道信息。

命令：*display dvpn session all*

例如：查看 Hub 设备上的隧道建立信息，如果有其中一台设备没有能与之建立起隧道信息，则将不会在信息中显示出来。其他 Hub 和 Spoke 设备与该设备之间均正常建立起了隧道。

```
<hub1>display dvpn session all
 Interface: Tunnel1   VPN name: 1   Total number: 3

  Private IP:      10.0.1.2
  Public IP:       192.168.1.2
  Session type:    Hub-Hub
  State:           SUCCESS
  Holding time: 0h 10m 15s
  Input:    81 packets,    80 data packets,    1 control packets
            73 multicasts,    0 errors
  Output: 83 packets,    82 data packets,    1 control packets
            71 multicasts,    0 errors

  Private IP:      10.0.1.3
  Public IP:       192.168.1.3
  Session type:    Hub-Spoke
  State:            SUCCESS
  Holding time:    0h 12m 4s
  Input:    98 packets,    97 data packets,    1 control packets
            89 multicasts,    0 errors
  Output: 106 packets,    105 data packets,    1 control packets
            90 multicasts,    0 errors
-------------------------------------------------------------
```

从 Spoke 设备检查隧道的建立情况时，要首先考虑 DVPN 的组网类型是属于哪一种。

DVPN 有两种典型的组网结构，Full-Mesh 网络和 Hub-Spoke 网络。

① Full-Mesh 网络中，Spoke 之间可以建立隧道直接通信，Hub 主要作为路由信息交换的中心。

② Hub-Spoke 网络中，Spoke 之间不能建立隧道直接通信，只能通过 Hub 转发数据，Hub 既作为路由信息交换的中心，又作为数据转发的中心。

命令：*display dvpn session all*

例如：在 Hub-Spoke 网络中，通过该命令检查，Spoke 与 Hub 之间建立起的隧道情况，当链路不通时，将无法建立。

```
[spoke1]display dvpn session all
 Interface: Tunnel1   VPN name: 1   Total number: 2

  Private IP:      10.0.1.2
  Public IP:       192.168.1.2
  Session type:    Spoke-Hub
  State:           SUCCESS
  Holding time:    0h 40m 2s
  Input:   258 packets,   257 data packets,   1 control packets
           252 multicasts,    0 errors
  Output: 727 packets,    726 data packets,   1 control packets
           250 multicasts, 0 errors

  Private IP:      10.0.1.1
  Public IP:       192.168.1.1
  Session type:    Spoke-Hub
  State:           SUCCESS
  Holding time: 0h 43m 3s
  Input:   299 packets,   298 data packets,   1 control packets
           281 multicasts,    0 errors
  Output: 291 packets,    290 data packets,   1 control packets
           280 multicasts, 0 errors
```

（7）检查 Hub 隧道配置

在 Hub 上需要检查隧道配置参数与其他 Hub 和 Spoke 上的隧道配置参数是否一致，对等体预共享密钥、安全协议验证算法、Tunnel 封装协议以及网络类型是否一致，如果不一致将会导致隧道无法建立起来。

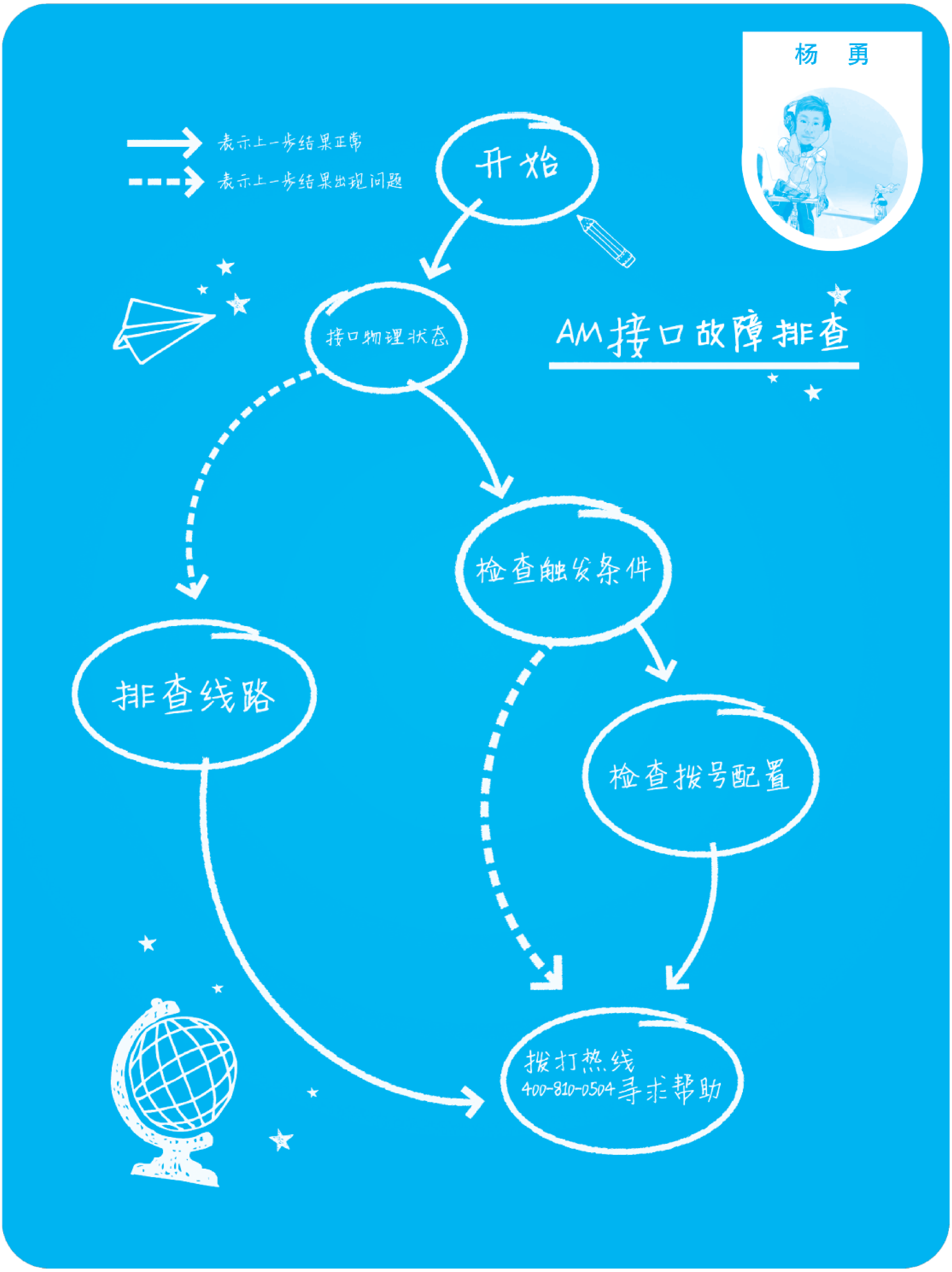
```
#
ike peer vam
 pre-shared-keyabcde                        //配置 IKE 对等体
#
ipsec transform-set vam                     //配置 IPSec 安全提议
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
#
ipsec profile vamp                          //配置 IPSec 安全框架
 pfs dh-group2
 ike-peer vam
 transform-set vam
 sa duration traffic-based 6000
#
interface Tunnel1
 ip address 10.0.1.1 255.255.255.0
 tunnel-protocol dvpn udp                   //隧道封装协议类型
 source GigabitEthernet0/0
 ospf network-type broadcast                //网络类型
 ipsec profile vamp
#
 vam client dvpn1hub1
```

(8) 检查 Spoke 隧道配置

在 Spoke 设备上检查隧道配置参数，需要考虑网络类型，如果是 Full-Mesh 类型的网络，需要检查与其他 Hub 和 Spoke 上的隧道配置参数是否一致；如果是 Spoke-Hub 网络类型，则只需要检查与对端 Hub 上隧道参数是否一致。然后检查对等体预共享密钥、安全协议验证算法、Tunnel 封装协议以及网络类型是否一致，如果不一致将会导致隧道无法建立起来。

```
#
ike peer vam                          //配置 IKE 对等体
 pre-shared-keyabcde
#
ipsec transform-set vam               //配置 IPSec 安全提议
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
#
ipsec profile vamp                    //配置 IPSec 安全框架
 pfs dh-group2
 ike-peer vam
 transform-set vam
 sa duration traffic-based 6000
#
interface Tunnel1
 ip address 10.0.1.3 255.255.255.0
 tunnel-protocol dvpn udp             //隧道封装协议类型
 source GigabitEthernet0/0
 ospf network-type broadcast          //网络类型
 ipsec profile vamp
 vam client dvpn1spoke1
#
```

杨 勇


表示上一步结果正常
表示上一步结果出现问题
开始
接口物理状态
AM接口故障排查
检查触发条件
排查线路
检查拨号配置
拨打热线
400-810-0504寻求帮助

1. 开始

AM 接口可实现模拟拨号用户的拨号接入/呼出功能，受线路及协议影响较大，定位故障的思路是：先查看物理层状态，检查线路连接，触发条件，之后排查设备配置。

2. 流程图相关操作说明

（1）接口物理状态

查看路由器上 AM 接口物理状态，确认其接口状态与协议是否 Up，AM 接口正常使用状态下其接口协议与当前状态都为 Up。

命令：*display interface analogmodem interface-number*

例如：通过命令查看路由器 AM2/0 当前状态 Up，协议 Up。

```
[H3C] display interface analogmodem 2/0
Analogmodem2/0 current state: Up
Line protocol current state: Up
Description: Analogmodem2/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 6.6.5.5/24 Primary
Link layer protocol is PPP
LCP opened, IPCP opened
```

如果 AM 接口当前状态为 Down，则查看面板指示灯是否闪烁，如果有闪烁则可确认报文已送到该 AM 接口；之后通过电话拨打测试，如果线路正常，则电话拨打可听到清楚的 Modem 拨号音。

（2）排查线路

选择正确的线缆类型。对于 PSTN 线路，可通过拨打电话方式进行测试：线路两端连接普通 PSTN 电话机，互相拨打测试，如果通话正常、无杂音，则将设备侧 PSTN 线路连接到 AM 接口，再次拨打测试。正常情况下，拨打 AM 接口可以听到清晰的 Modem 拨号音。

（3）检查触发条件

AM 接口拨号应用中需配置感兴趣数据流触发接口拨号，当无符合的匹配条件数据流经过时，AM 接口状态为 Down。检查设备 dialer-rule 配置，如使用 ACL 来匹配数据流，可使用 display acl all 命令查看匹配项。

例如：使用 display acl all 查看 ACL number 为 2000 的规则是否有报文匹配，显示信息中为有 2 次匹配。

```
[H3C] display acl all
Basic ACL  2000, named flow,1 rules,
This is an IPv4 basic ACL.
Statistics is enabled
ACL's

step is 5
rule0 permit source 1.1.1.1 0 (2 times matched)
```

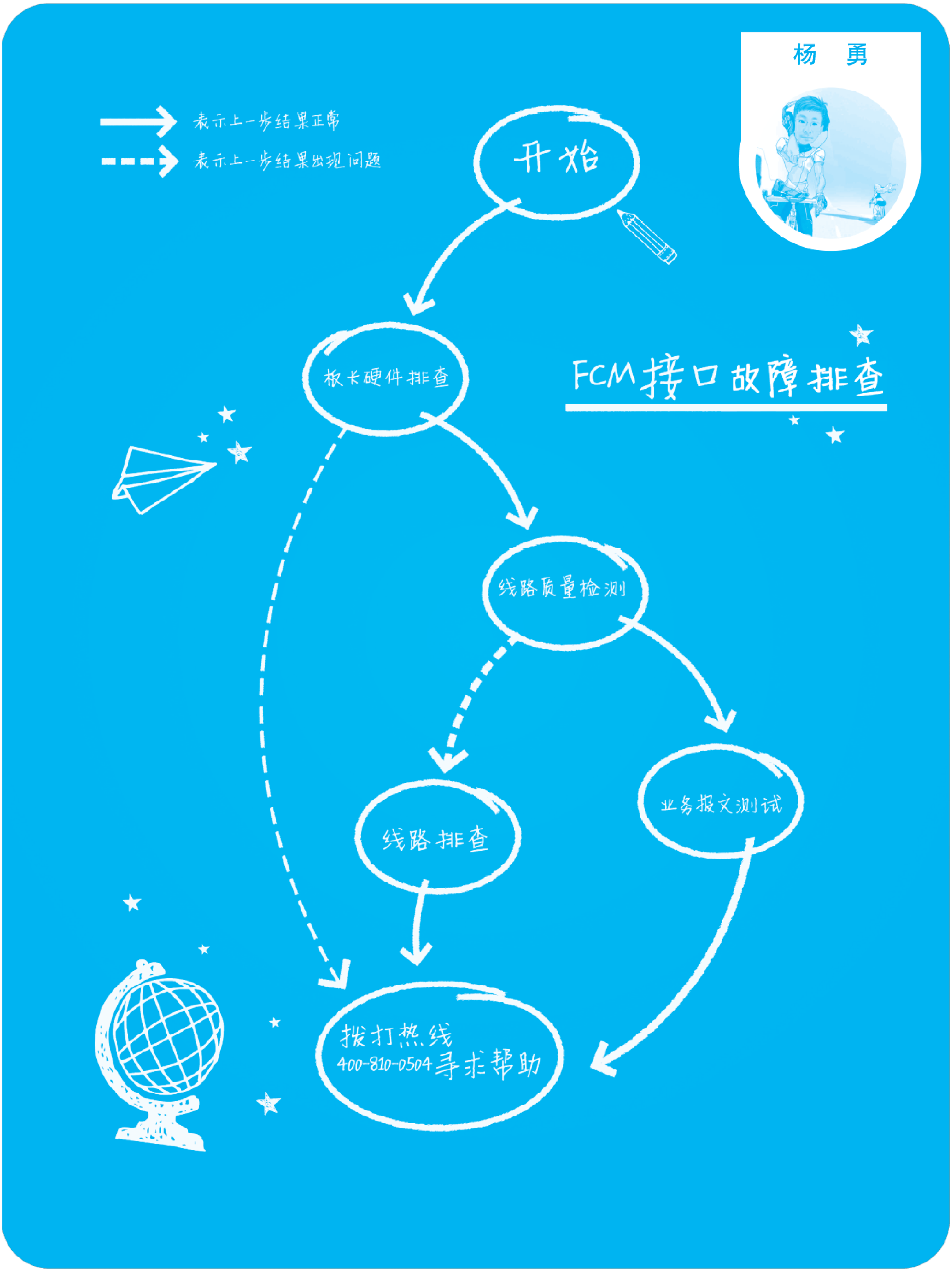
（4）检查配置

AM接口主要应用于拨号，检查配置应关注与AM接口的相对应的TTY虚接口是否启动Modem的呼入与呼出、拨号使用的被叫号码、验证方式及用户名密码等DCC拨号相关配置。

命令：*display current-configuration*

例如：在设备上通过display current-configuration查看配置是否正确。

```
[H3C]display current-configuration
#
interface Analogmodem5/9
 async mode protocol
 link-protocol ppp
 dialer enable-circular
 dialer circular-group 1                    //绑定拨号组
#
interface Dialer1
 link-protocol ppp
 ppp pap local-user h3c password simple h3c  //配置用户名与密码
 ip address 12.1.1.2 255.255.255.0
 dialer enable-circular                     //配置拨号方式
 dialer-group 1                             //配置拨号组
 dialer route ip 12.1.1.1 1427              //配置号码路由
#
 ip route-static 0.0.0.0 0.0.0.0 Dialer1    //配置拨号后路由
#
 dialer-rule 1 ip permit                    //配置触发条件
#
user-interface tty 81 92                    //配置 Modem 的呼叫呼入与呼出
modem call-both
```


杨 勇
表示上一步结果正常
表示上一步结果出现问题
开始
FCM接口故障排查
板卡硬件排查
线路质量检测
线路排查
业务报文测试
拨打热线
400-810-0504寻求帮助

1. 开始

FCM 板卡承载金融 POS 机刷卡交易业务,使用中出现的问题一般与线路及业务报文关系较大,定位故障的思路是:先查接口硬件,之后查线路连通性与质量,最后排查交易报文是否正常。

2. 流程图相关操作说明

(1) 板卡硬件排查

首先从 POS 机侧确认故障现象,交易业务是否成功,即 POS 机是否能正确完成查询、消费等业务,之后 FCM 接口状态与接口对应 Terminal ID 的报文收发统计信息。

命令: *display posa status terminal*

例如: 显示 FCM5/0 接口 Up 处于连接状态,注意只有接口正在交易时 FCM 接口才会 Up。

```
[H3C] display posa status terminal
TerminalID  Type     Interface     ListenPort        State
1           TCP      -             2000              linked
2           FCM      fcm5/0        -                 Up
```

命令: *display posa statistics terminal*

例如: 查看 Terminal ID 为 2 的接口收发报文一致,无错包,无链路丢包。

```
[H3C] display posa statistics terminal
TerminalID  Receive  Send  PktErr  DisErr  InDiscarded  OutDiscarded
1           100      100   0       0       0            0
2           60       60    0       0       0            0
```

如果报文统计发生异常,连接无法 Up,则需通过如下测试方法判断是否硬件问题导致。

当 POS 机侧进行交易时,查看 FCM 单板指示灯是否闪烁,如果指示灯没有亮,则有可能是线路或板卡硬件问题,此时可以将 FCM 侧与 POS 侧更换为普通 PSTN 电话机,拨打测试,确认是否可以互通,如果可以互通则可判断为设备侧问题。

(2) 线路质量测试

查看接口信息中错包统计,错包率较高,则可能为线路质量较差造成,此时会影响交易的成功率。

命令: *display interface fcm interface-number*

例如: 只有在有交易时,该接口物理才会 Up,否则是 Down 的状态。

```
[H3C]display interface fcm6/0
Fcm6/0 current state: Down
Line protocol current state: Down
Description: Fcm6/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
```

```
LCP initial
    Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
    Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
    Input: 0 packets, 0 bytes
           0 broadcasts, 0 multicasts
           0 errors,0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
    Output:0 packets, 0 bytes
           0 errors,0 underruns, 0 collisions
    0 deferred
```

（3）线路测试

线路测试方法为：两端接电话机，互拨通话后，确认是否存在杂音；FCM 接口连接线路，POS 机侧电话拨打，确认是否可以听到清晰的 Modem 拨号音，如果通话存在杂音，无法听到清晰的 Modem 音，则可确认线路质量存在问题。线路测试需要多次拨打，并保证现象一致。

（4）业务报文测试

路由器收不到 POS 机发送的报文，可以通过如下方式排查，设备开启 debugging posa all 开关，POS 侧进行交易，查看 debug 信息中是否有接口的 POS 交易报文。POS 业务交易报文流程比较简单，每一笔业务交易需要四个报文。

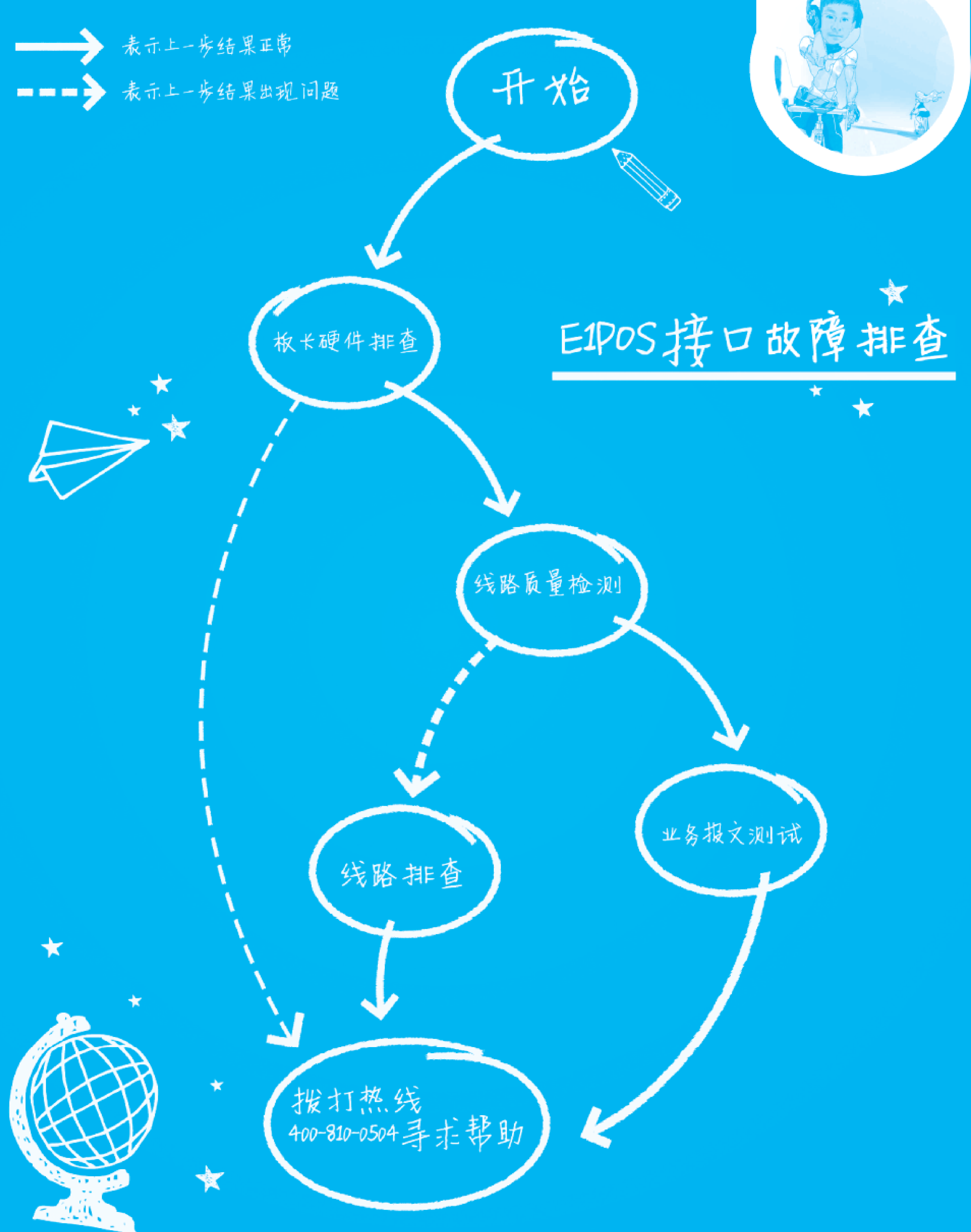
命令：*debugging posa all*

例如：FCM5/3 接口对应 Terminal 4 接口的报文交互过程如下。

```
%Jul  6 13:02:29:269 2011 MSR50 IFNET/3/LINK_UPDOWN: Fcm5/3link status is Up.  //收到呼叫,接口 Up
 *Jul  6 13:02:29:269 2011 MSR50 POSA/7/EVENT:
Received IOCtrl(1) message from line(84).
 *Jul  6 13:02:29:270 2011   MSR50   POSA/7/EVENT:
Terminal 4: Received line up message.
Received 300 bytes from fcm terminal 4          //收到 POS 机发来的报文
ID(0x60) DST(0x0003) SRC(0x0000)
 Total length: 300 Offset: 0, partial data as follows:
 0x000: 60 00 03 00 00 13 04 08 00 20 20 01 00 00 c0 00
 0x010: 08 99 00 00 00 03 70 00 18 33 32 30 30 30 30 30
 *Jun 28 09:49:10:851 2011 MSR50 POSA/7/EVENT:
App 1: Succeeded to send connecting request to server.
Sent 302 bytes to tcp application 1.                  //发送给前置机
 PktLen(0x012c) ID(0x60) DST(0x0003) SRC(0x0004)
 Total length: 302 Offset: 0, partial data as follows:
 0x000: 01 2c 60 00 03 00 04 13 04 08 00 20 20 01 00 00
 0x010: c0 00 08 99 00 00 00 03 70 00 18 33 32 30 30 30
 *Jun 28 09:49:10:854 2011 MSR50-40 POSA/7/EVENT:
App 1: Received ASYN_READ message from socket(1).
 *Jun 28 09:49:10:854 2011 MSR50-40 POSA/7/PACKET:
Received 353 bytes from tcp application 1.            //收到前置机的回应报文
 PktLen(0x0161) ID(0x60) DST(0x0004) SRC(0x0003)
 Total length: 353 Offset: 0, partial data as follows:
 0x000: 01 61 60 00 04 00 03   13 04 08 10 20 38 01 00 02
 0x010: c1 01 08 99 00 00 00 03 70 17 34 10 02 22 00 18
 *Jun 28 09:49:10:954 2011 MSR50 POSA/7/PACKET:
```

```
Sent 351 bytes to fcm terminal 4.                    //发送给 POS 机
 ID(0x60) DST(0x0000) SRC(0x0003)
 Total length: 351 Offset: 0, partial data as follows:
 0x000: 60 00 00 00 03 13 04 08 10 20 38 01 00 02 c1 01
 0x010: 08 99 00 00 00 03 70 17 34 10 02 22 00 18 30 30
%Jul  6 13:03:04:075 2011 MSR50 IFNET/3/LINK_UPDOWN: Fcm5/3 link status is Down.//POS 机挂断
 *Jun 28 09:49:23:647 2011 MSR50 POSA/7/EVENT:
Terminal 4: Received IOCtrl(2) message from line(84) Object-Type(1) Index(5308659) If-Type(89).
 *Jun 28 09:49:23:647 2011 MSR50-40 POSA/7/EVENT:
Terminal 4: Received line down message.
```

杨 勇



表示上一步结果正常
表示上一步结果出现问题
开始
E1POS接口故障排查
板卡硬件排查
线路质量检测
线路排查
业务报文测试
拨打热线
400-810-0504寻求帮助

1. 开始

E1POS 问题故障现象多表现为刷卡失败率高、冲正率高、POS 机侧交易超时等，此类问题多与线路质量相关，定位故障的思路是：首先查板卡硬件，之后排查线路质量，最后检查业务交易报文。

2. 流程图相关操作说明

(1) 板卡硬件排查

通过命令查看接口连接状态，及接口时隙下错包，判断线路质量及板卡是否有问题。板卡接口在存在交易时候接口无法 Up，则可能为板卡硬件问题；接口存在大量错误报文则与线路及板卡硬件相关，需进一步排查。

命令：*display posa status terminal*

display interface fcm interface-number

例如：查看接口连接状态 Up，及对应时隙下无错包。

```
[H3C] display posa  status terminal
TerminalID    Type    Interface          ListenPort   State
1             FCM     Fcm5/0:15.0        -            Up
31            FCM     Fcm8/0:15.0        -            Up

[H3C] display interface Fcm5/0:15.0
Fcm5/0:15.0 current state: Down
Line protocol current state: Down
Description: Fcm5/0:15.0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
 Last clearing of counters:   10:28:40 Fri 04/26/2013
    Last 300 seconds input rate 0.00 bytes/sec, 0.00 packets/sec
    Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
    Input: 0 packets, 0 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
           1 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
    Output:0 packets, 0 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
```

(2) 线路质量检测

E1POS 板卡要求运营商线路使用无损编解码方式，推荐使用 TDM 交换，使用 G.711 无损编码，使用 G723、G729 等有损编码容易造成交易失败，对于线路质量可通过命令查看接口时隙报文统计与电话拨打测试方式排查。

命令：*display posa statistics terminal*

例如：显示 POS 接口和应用收到和发送了正确的报文，没有错误的报文，表明业务正常。

```
[H3C] display posa statistics terminal
TerminalID  Receive  Send  PktErr  MapErr  InDiscarded  OutDiscarded
1           1        1     0       0       0            0
2           1        1     0       0       0            0
```

将 POS 机更换为电话，拨打接入号码，要求在 10 秒内可听到清晰的 Modem 音。

(3) 线路排查

通过拨打电话方式测试，要求在 10 秒内可听到清晰的 Modem 音，也可以抓取单板侧 PCM 报文确认。

(4) 业务报文测试

路由器收不到 POS 机发送的报文，可以通过如下方式排查，设备开启 debugging posa all 开关，POS 侧进行交易，查看 debug 信息中是否有接口的 POS 交易报文，或根据主叫号码抓取 POS 业务交易报文。

命令：*debugging posa all*

例如：Fcm10/0:15.8 对应 Terminal 9 的报文交互过程。

```
%May  4 15:57:29:212 2012 H3C IFNET/3/LINK_UPDOWN: Fcm10/0:15.8link status is Up.
                                                   //收到呼叫,接口 Up
*May  4 15:57:29:212 2012 H3C POSA/7/EVENT:
Terminal 9: Received IOCtrl(1) message from line(505) Object-Type(1) Index(51364a) If-Type(81).
*May  4 15:57:29:212 2012 H3C POSA/7/EVENT:
Terminal 9: Received line up message.
*May  4 15:57:29:212 2012 H3C POSA/7/EVENT:
Terminal 9:Get FCM terminal caller-ID:5575113           //获取主叫号码
*May  4 15:57:31:705 2012 H3C POSA/7/EVENT:
Received data from interface(5322314).
*May  4 15:57:31:705 2012 H3C POSA/7/PACKET:
Received 196 bytes from fcm terminal 9.                 //收到 POS 机发来的报文
 ID(0x60) DST(0x0100) SRC(0x0000)
 Total length: 196 Offset: 0, partial data as follows:
 0x000: 60 01 00 00 00 01 00 00 30 35 38 35 30 31 37 34
 0x010: 00 00 00 00 00 00 00 00 ab 02 00 20 10 20 12 04
*May  4 15:57:31:705 2012 H3C POSA/7/EVENT:
Terminal 9: Received line data message.
*May  4 15:57:31:705 2012 H3C POSA/7/PACKET:
Sent 231 bytes to tcp application 1.                    //发送给前置机
 PktLen(0x00e5) ID(0x60) DST(0x0100) SRC(0x0009)
 Total length: 231 Offset: 0, partial data as follows:
 0x000: 00 e5 60 01 00 00 09 4c 52 49 00 1c 00 00 00 00
 0x010: 05 57 51 13 00 00 00 00 00 00 00 00 00 00 00 00
*May  4 15:57:34:752 2012 H3C POSA/7/EVENT:
App 1: Received ASYN_READ message from socket(1).
*May  4 15:57:34:752 2012 H3C POSA/7/PACKET:
Received 269 bytes from tcp application 1.              //收到前置机的回应报文
 PktLen(0x010b) ID(0x60) DST(0x0009) SRC(0x0100)
 Total length: 269 Offset: 0, partial data as follows:
 0x000: 01 0b 60 00 09 01 00 01 00 23 35 35 37 35 31 31
 0x010: 33 20 20 20 20 20 20 20 20 00 f2 02 00 38 30 31
*May  4 15:57:34:752 2012 H3C POSA/7/PACKET:
Sent 267 bytes to fcm terminal 9.                       //发送给 POS 机
```

```
ID(0x60) DST(0x0000) SRC(0x0100)
 Total length: 267 Offset: 0, partial data as follows:
 0x000: 60 00 00 01 00 01 00 23 35 35 37 35 31 31 33 20
 0x010: 20 20 20 20 20 20 20 00 f2 02 00 38 30 31 38 31
%May  415:57:37:457 2012 H3C IFNET/3/LINK_UPDOWN: Fcm10/0:15.8 link status is Down.
//POS 机挂断
 * May  4 15:57:37:458 2012 H3C POSA/7/EVENT:
Terminal 9: Received IOCtrl(2) message from line(505) Object-Type(1) Index(51364a) If-Type(81).
 * May  4 15:57:37:458 2012 H3C POSA/7/EVENT:
Terminal 9: Received line down message.
```


马文斌
表示上一步结果正常
表示上一步结果出现问题
开始
检查匹配项配置
拥塞管理故障排查
查看接口队列统计
接口是否拥塞
检查接口速率与线路带宽是否匹配
拨打热线400-810-0504寻求帮助

02 路由技术 > 2.6 QoS > 拥塞管理故障排查 > 步骤详解

1. 开始

由于拥塞管理使用的是队列技术，进入队列的前提必须要符合匹配项。定位故障的思路是：先检查匹配项是否正确，再检查接口队列信息，再检查接口是否拥塞，最后检查接口速率和链路带宽是否匹配。

2. 流程图相关操作说明

（1）查看匹配项是否正确

查看进入各个队列的匹配项是否正确，匹配项不正确，会导致相应的流量无法进入队列。

命令：PQ 队列：*display qos pql X*

CQ 队列：*display qos cql X*

CBQ 队列：*display qos interface interface-type interface-number*

例如：以 PQ 为例，匹配 ACL 2000 的数据进入 Top 队列，从 GigabitEthernet0/1 进入的报文进入 Middle 队列，mpls exp 等于 5 的报文进入 Bottom 队列。

```
[H3C]display qos pql 1
Current PQL Configuration:
List   Queue    Params
------------------------------------------------------
1      Top      Protocol ip acl 2000
1      Middle   Inbound-interface GigabitEthernet0/1
1      Bottom   Protocol mpls exp 5
```

（2）查看接口队列统计信息

查看接口下的队列是否已经有报文进入。

命令：

PQ 队列：*display qos pq interface interface-type interface-number*

默认队列为 *normal*。

CQ 队列：*display qos cq interface interface-type interface-number*

默认进入队列 1。

CBQ 队列：*display qos cbq interface interface-type interface-number*

默认进入 BE 队列。

例如：通过命令查看 PQ 队列，可以确认接口已经产生拥塞，并且报文已经进入队列。

```
[H3C]display qos pq interface g0/0
Interface: GigabitEthernet0/0
Output queue : (Urgent queuing : Size/Length/Discards)   0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)   0/500/0
Output queue : (Priority queuing : PQL 1 Size/Length/Discards)
Top:   2/20/0     Middle:   3/40/0     Normal:   60/60/2     Bottom:   0/80/0
```

（3）检查接口是否拥塞

使用如下命令查看当前接口流量是否已经超过了链路带宽。

命令：*display interface interface-type interface-number*

通过命令可以看到当前 GigabitEthernet 0/0 接口流量。

```
[H3C]display interface GigabitEthernet  0/0
GigabitEthernet0/0
Current state: Up
Line protocol state: Up
Description: GigabitEthernet0/0 Interface
...
Last clearing of counters: Never
Last 300 seconds input rate: 486.73 bytes/sec, 3893 bits/sec, 4.96 packets/sec
Last 300 seconds output rate: 486.73 bytes/sec, 3893 bits/sec, 4.96 packets/sec
```

（4）查看接口速率和链路带宽是否匹配

普通以太接口默认的带宽都是百兆或千兆，但是实际带宽都要小于接口带宽，接口拥塞依靠的是接口的带宽，所以需要使用接口限速方法将接口带宽控制在实际带宽。如果接口速率已经和链路带宽相匹配，则不用检查。

命令：*display qos lr interface interface-type interface-number*

例如：在接口 G0/0 使用接口限速，使用命令查看，可以看到，当前接口被限速为 8Kbps。

```
[H3C]display qos lr interface GigabitEthernet 0/0
Interface: GigabitEthernet0/0
 Direction: Outbound
 CIR 8 (Kbps),  CBS 500 (byte),  EBS 0 (byte)
 Passed : 27(Packets) 25710(Bytes)
 Delayed: 15(Packets) 19062(Bytes)
 Active Shaping: YES
```

（5）查看当前流量是否超过链路带宽

因为拥塞管理在接口拥塞状态下，队列才会生效，所以接口当前带宽超过了 LR 限制的带宽时，拥塞管理才会生效，命令同上。

例如：通过命令可看到，Active Shaping 变为了 YES，说明当前接口流量已经超过了 LR 限速。

```
[H3C]display qos lr interface GigabitEthernet 0/0
Interface: GigabitEthernet0/0
 Direction: Outbound
 CIR 8 (kbps),  CBS 500 (byte),  EBS 0 (byte)
 Passed : 27(Packets) 25710(Bytes)
 Delayed: 15(Packets) 19062(Bytes)
 Active Shaping: YES
```


终端通过H323无法注册故障排查
马文斌
开始
查看配置
排查网络
排查服务器是否回复报文
服务器回复异常报文，在网关和网守同时抓包
拨打热线400-810-0504寻求帮助
表示上一步结果正常
表示上一步结果出现问题

02 路由技术 › 2.7 VoIP › 2.7.1 终端通过 H323 无法注册故障排查 › 步骤详解

1. 开始

终端无法通过 H323 注册问题的排错思路为：先查看配置，再查看网络，然后在排查服务器侧能否正常回应请求报文。

2. 流程图相关操作说明

（1）查看配置

查看 MSR 路由器上的语音相关配置是否正确，查看配置有如下关键点。

① 查看路由器是否配置语音网关使用的源 IP 地址。

② 查看路由器是否配置网关别名。

③ 查看路由是否配置网管对应的主用网守名称和 IP 地址。

④ 查看路由器是否激活 GK Client 功能。

⑤ 查看路由器是否有可注册实体。

查看路由器是否开启注册功能。

命令：进入 *voice-setup* 视图下使用 *display this* 命令

例如：通过命令查看，可以看到主用 GK 的名字为 gk-server，地址为 172.31.123.13，端口为 1719；备用 GK 的 gk-server 名字为 gk-server-slave，地址为 172.31.123.14，端口为 1719，；本端注册使用的源地址为 1.1.1.9；本端的网关名称为 h3c；开启了注册功能。

```
[H3C]voice-setup                                    //进入 voice-setup 视图
[H3C-voice]display this
#
voice-setup
 #
gk-client
  gk-id gk-server gk-addr 172.31.123.13 1719  //要和 GK 的 gk-name 一致
  gk-2nd-id gk-server-slave gk-addr 172.31.123.14 1719
  gw-address 1.1.1.9                          //一般使用路由的 loopback 接口
  gw-id h3c                                   //要和 GK 上配置的 gw-id 一致
  ras-on                                      //开启注册功能
#
```

查看路由器是否有可注册实体，可注册实体要求如下。

① 必须为 Pots 实体。

② Pots 实体下必须要配置 Match-Template。

③ 实体下没有配置 Undo Register-Number 命令。

命令：进入 *dial-program* 视图，使用 *display this* 命令

例如：通过命令可以看到存在可注册实体 1000。

```
[H3C]voice-setup                    //进入 voice-setup 视图
[H3C-voice] dial-program            //进入 dial-program 视图
[H3C-voice-dial]display this
#
```

```
#
 dial-program
  #
  entity 1000 pots
   match-template 1000
   line 1/0
#
return
```

(2) 排查网络

查看终端设备和 SIP 服务器之间是否可达包括以下两方面。

① 终端和 H323 服务器之间路由可达。

② 终端和 H323 服务器之间 1719(注册端口)和 1720(建立会话端口)端口可达。

查看终端和路由器之间是否路由可达。

命令:*ping x.x.x.x*

例如:通过命令查看,可以确认终端和 SIP 服务器之间路由可达。

```
[H3C]ping 172.31.123.13
  PING 172.31.123.13: 56  data bytes, press CTRL_C to break
    Reply from 172.31.123.13: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 172.31.123.13: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.31.123.13: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.31.123.13: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.31.123.13: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 172.31.123.13 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

路由可达后需要再查看路由器和 H323 服务器之间 1719 端口是否可达。

需要服务器侧配合查看是否能够收到路由器发出的请求报文,如果服务器侧无法收到,请排查网络中是否存在防火墙,如果存在防火墙,请放通相应的协议和端口,如果不存在防火墙,请排查协议报文丢在网络哪个位置。

(3) 排查服务器是否回复报文

需要协调服务器侧人员查看收到我司发出的 H323 请求报文后,服务器是否能够回应,如果服务器侧没有回应请协调服务器侧处理。

(4) 服务器回复异常消息

可通过 debugging 命令来查看服务器回复的消息类型,通过服务器回复的类型,可大致判断问题可能性。

命令:*debugging voice ipp all*

terminal debugging

terminal monitor

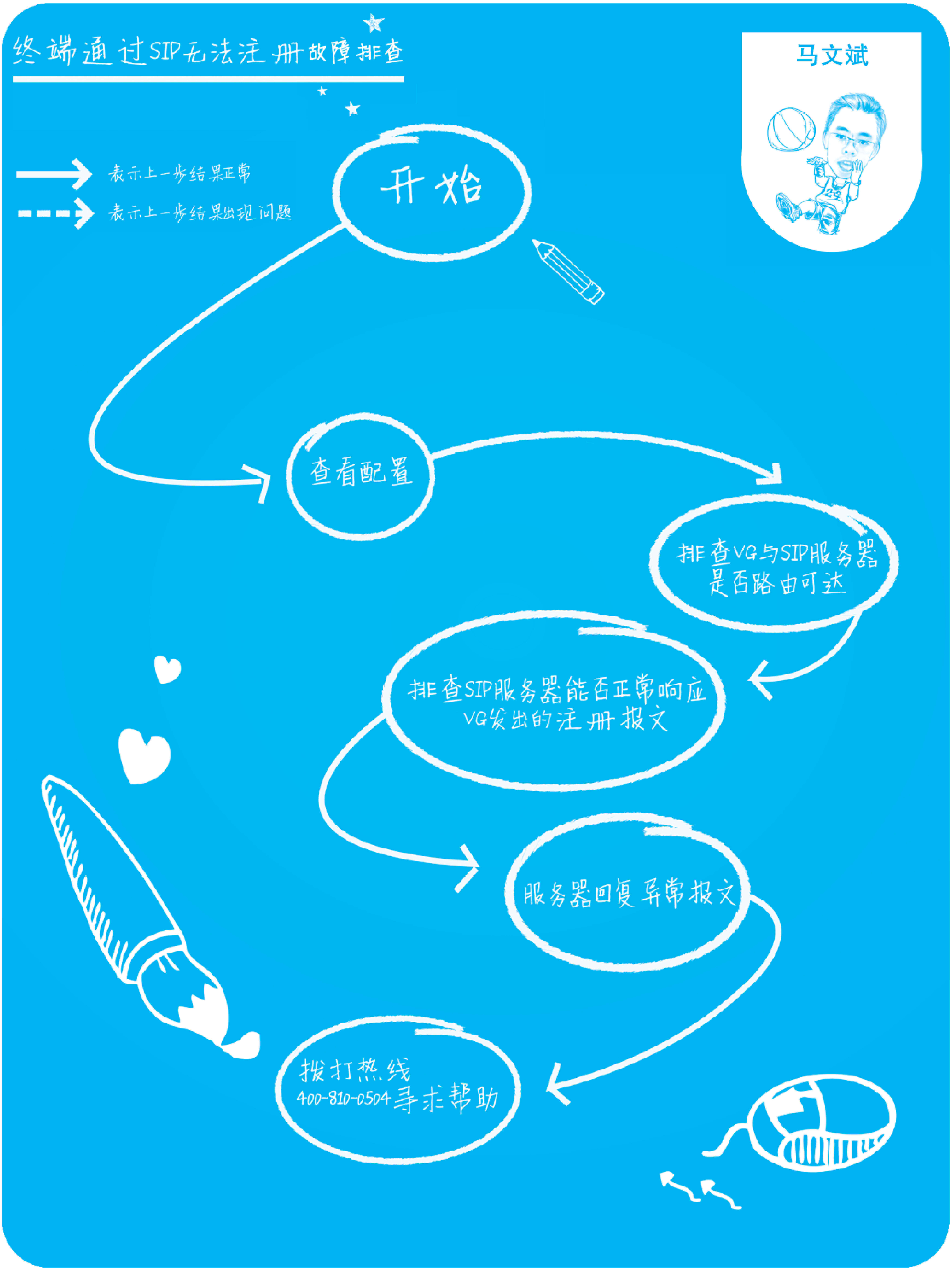
例如:通过如上命令可以查看到路由器向 GK 网关 172.31.123.13 发送 RRQ 注册报文,然后收到了服务回复的 RCF,表示注册成功。若 GK 回复 RRJ 消息,则说明服务器拒绝网关注册,确定路由器配置无误后,需要协调服务器侧排查为什么拒绝注册。

```
* Dec 25 16:13:02:452 2013 5 IPP/7/VOICE:
  IPP_RAS [SYS]:Send heavy RRQ (4) Msg to GK (172.31.123.13) when receive GCF Msg
                                        //VG 向 GK(172.31.123.13)发送 RRQ 注册报文

* Dec 25 16:13:02:452 2013 5 IPP/7/VOICE:
  IPP_SOK [SYS]:Send a RAS Msg on Socket = 27 ,length = 75

* Dec 25 16:13:02:468 2013 5 IPP/7/VOICE:
  IPP_SOK [SYS]: Receive Socket Msg ASYN_READ sockid = 27

* Dec 25 16:13:02:469 2013 5 IPP/7/VOICE:
  IPP_RAS [SYS]:Receive RCF Msg, Seq=4, TTL=180       //收到 GK 回复的 RCF 消息,说明
                                                      //VG 已经注册成功
```


终端通过SIP无法注册故障排查
马文斌
表示上一步结果正常
表示上一步结果出现问题
开始
查看配置
排查VG与SIP服务器是否路由可达
排查SIP服务器能否正常响应VG发出的注册报文
服务器回复异常报文
拨打热线
400-810-0504寻求帮助

02 路由技术 ▶ 2.7 VoIP ▶ 2.7.2 终端通过 SIP 无法注册故障排查 ▶ 步骤详解

1. 开始

终端无法通过 SIP 注册问题的排错思路为：先查看配置，再查看网络，然后再排查服务器侧能否正常回应 SIP 请求报文。

2. 流程图相关操作说明

（1）查看配置

查看 MSR 路由器上的语音相关配置是否正确，查看配置有两个关键点：①查看路由器是否开启 SIP 注册功能；②查看路由器是否有可注册实体。

查看路由器是否开启注册功能。

命令：进入 *SIP* 视图下使用 *display this* 命令

例如：通过命令查看，当前主用的 SIP 服务器地址为 172.31.123.121；备用 sip 服务器地址为 172.31.123.123；当前开了 SIP 注册功能。

```
[H3C]voice-setup                          //进入 voice-setup 视图
[H3C-voice]sip                            //进入 SIP 视图
[H3C-voice-sip]display this
#
 #
 sip
  registrar ipv4 172.31.123.121           //主用 SIP 服务器地址
  registrar ipv4 172.31.123.123 slave     //备用 SIP 服务器地址
  register-enable on                      //开启注册功能
#
return
```

查看路由器是否有可注册实体，可注册实体要求：①必须为 Pots 实体；②Pots 实体下必须配置 Match-Template；③实体下没有配置 Undo Register-Number 命令。

命令：进入 *dial-program* 视图，使用 *display this* 命令

例如：通过命令可以看到存在可注册实体 4000。

```
[H3C]voice-setup               //进入 voice-setup 视图
[H3C-voice] dial-program       //进入 dial-program 视图
[H3C-voice-dial]display this
#
 #
 dial-program
  #
  entity4000 pots
   match-template4000          //需要注册的号码
   line 1/0                    //此实体对应的接口
#
return
```

（2）排查 VG 与 SIP 服务器是否路由可达

查看终端设备和 SIP 服务器之间是否可达包括两方面：①终端和 SIP 服务器之间路由可

达；②终端和 SIP 服务器之间 5060 端口可达。

查看终端和路由器之间是否路由可达。

命令：*ping x.x.x.x*

例如：通过命令查看，可以确认终端和 SIP 服务器之间路由可达。

```
[H3C]ping 172.31.123.121
  PING 172.31.123.121: 56   data bytes, press CTRL_C to break
    Reply from 172.31.123.121: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 172.31.123.121: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.31.123.121: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.31.123.121: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.31.123.121: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 172.31.123.121 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

路由可达后需要再查看路由器和 SIP 服务器之间 5060 端口是否可达。

需要服务器侧配合查看是否能够收到路由器发出的请求报文，如果服务器侧无法收到，请排查网络中是否存在防火墙，如果存在防火墙，请放通相应的协议和端口，如果不存在防火墙，请排查协议报文丢在网络哪个位置。

MSR 路由器 SIP 默认基于 UDP，使用默认端口为 UDP，可更改。

可选基于 TCP 和 TLS。

命令：进入 SIP 视图下使用 *display this* 命令

例如：通过如上命令可以查看到主用服务器基于 TCP、端口号使用 50000 的 SIP 协议；备用服务器使用默认，基于 UDP，端口号为 5060 的 SIP 协议。

说明：VG 上使用的注册端口取决于 SIP 服务器，若 SIP 服务器没有做特殊设置，那么请使用标准的 5060 端口，若 SIP 服务器要求使用特殊端口，则 VG 侧需要配合 SIP 服务器做更改。

```
[H3C]voice-setup
[H3C-voice]sip
[H3C-voice-sip]display this
#
 sip
  registrar ipv4 172.31.123.121 port 50000 tcp
  registrar ipv4 172.31.123.123 port 5060 slave
  register-enable on
#
return
```

(3) 排查 SIP 服务器是否回正常响应 VG 发出的注册报文

需要协调服务器侧人员查看收到我司发出的 SIP 请求报文后，服务器是否能够回应 200 OK 或者 401 鉴权消息，如果服务器侧没有回应请协调服务器侧处理。

说明：200 OK 消息代表服务器同意注册并返回注册成功消息；401 消息代表服务器同意注册，但是需要 VG 上送鉴权消息(注册的用户名密码等)，VG 重新发送带有鉴权消息的注册

报文，如果鉴权通过，则服务器回复 200 OK 消息告知 VG 注册成功。

(4) 查看服务器回复异常报文

可通过 *debugging* 命令来查看服务器回复的消息类型，通过服务器回复的类型，可大致判断问题可能性。

命令：*debugging voice sip message*

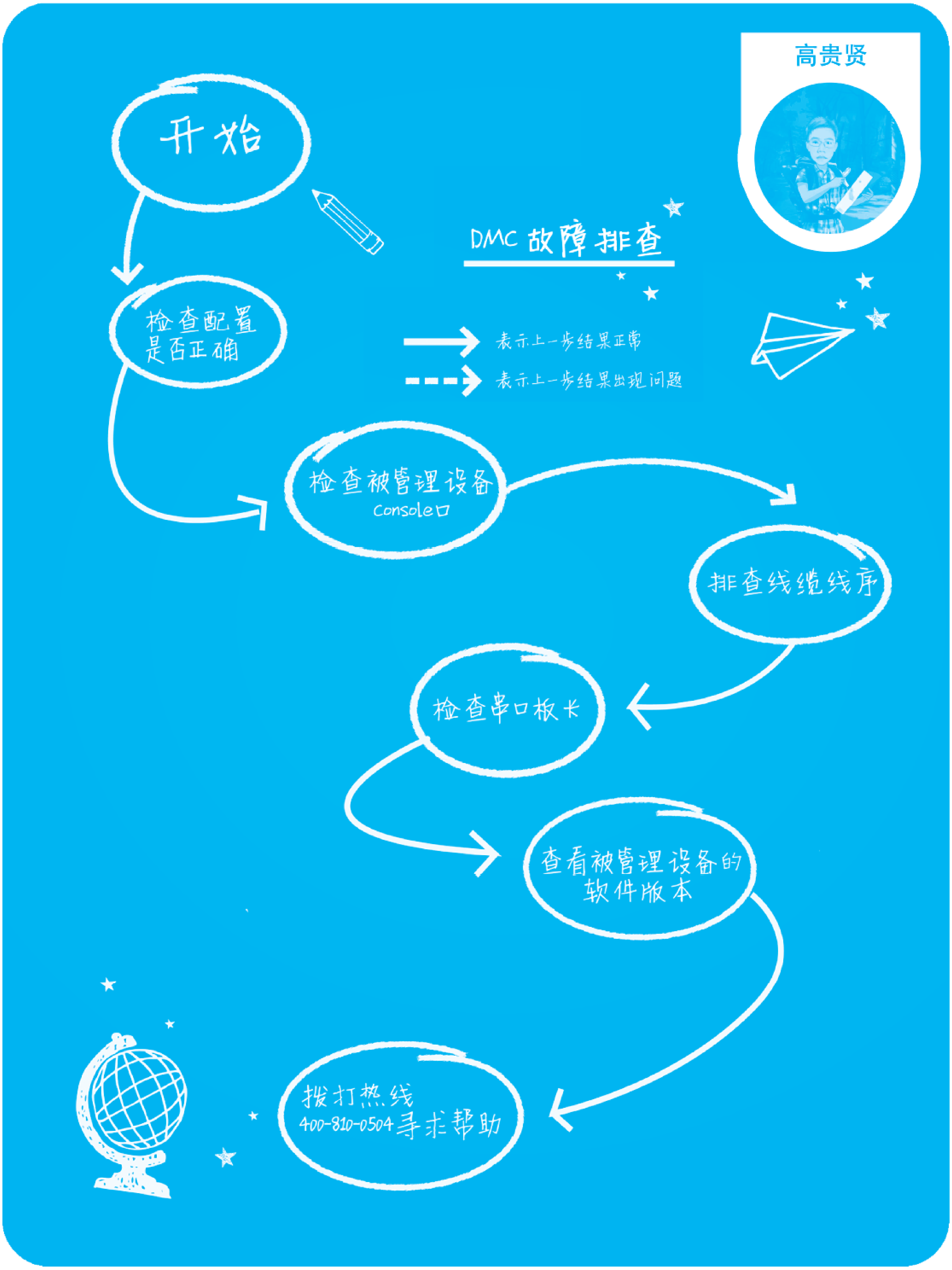
terminal debugging

terminal monitor

例如：通过如上 deb 可查看到路由器向 SIP 服务器发出注册消息，本地地址为 172.31.123.19，SIP 服务器地址为 172.32.123.121，注册的号码为 4000；服务器回复了 200 OK 报文，注册成功。

```
*Dec 25 15:20:32:666 2013 5 SIP/7/VOICE:
Stack--->NetWork:                //路由器向外发出 SIP 注册消息
REGISTER sip:172.31.123.121:5060 SIP/2.0
Via: SIP/2.0/UDP 172.31.123.19:5060;branch=z9hG4bKf10253b3bf2
Call-ID: 5e5a0cc9ae20da542b5b2bd4c7db3398@172.31.123.19
From: <sip:4000@172.31.123.121>;tag=bf2e990c
To: <sip:4000@172.31.123.121>
CSeq: 1 REGISTER
Contact: <sip:4000@172.31.123.19:5060>
Expires: 3600
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER, INFO, PRACK, SUBSCRIBE,
NOTIFY,UPDATE,REFER
Date: Wed, 25 Dec 2013 15:20:32 GMT
Max-Forwards: 70
Supported: timer
Content-Length: 0

*Dec 25 15:20:32:714 2013 5 SIP/7/VOICE:
NetWork--->Stack:          //路由器收到服务器回复的报文
SIP/2.0 200 OK             //200 OK 表示注册成功
via: SIP/2.0/UDP 172.31.123.19:5060;branch=z9hG4bKf10253b3bf2
from: <sip:4000@172.31.123.121>;tag=bf2e990c
to: <sip:4000@172.31.123.121>;tag=a4f0763c
call-id: 5e5a0cc9ae20da542b5b2bd4c7db3398@172.31.123.19
cseq: 1 REGISTER
date: Wed, 25 Dec 2013 07:03:19 GMT
contact: <sip:4000@172.31.123.19:5060>
allow: INVITE, ACK, BYE, CANCEL, REFER, SUBSCRIBE, NOTIFY, PRACK, UPDATE,
OPTIONS,MESSAGE,FEATURE
supported: timer
expires: 3600
user-agent: 3Com VCX 7210 IP CallProcessor/v10.0.8
content-length: 0
```


高贵贤
开始
DMC 故障排查
检查配置是否正确
表示上一步结果正常
表示上一步结果出现问题
检查被管理设备Console口
排查线缆线序
检查串口板卡
查看被管理设备的软件版本
拨打热线
400-810-0504寻求帮助

02 路由技术 ＞ 2.8 DMC ＞ DMC 故障排查 ＞ 步骤详解

1. 开始

DMC 的故障问题多为无法正确识别设备，故障定位思路为：检查配置是否正确、检查被管理设备 Console 口、排查线缆线序、检查串口板卡、查看被管理设备的软件版本。

2. 流程图相关操作说明

（1）检查配置是否正确

查看配置包括全局下是否使能 DMC 功能、接口以及 TTY 下的相应配置、TTY 的标号。

命令：*display user-interface*

display current-configuration

```
[DMC]display   user-interface
   Idx   Type      Tx/Rx        Modem Privi   Auth   Int
   81    TTY 81    9600         -        0     N      Asy5/0

[DMC]display current-configuration
#
dmc enable
#
interface Async5/0
 async mode flow
 undo detect dsr-dtr
 link-protocol ppp
#
user-interface tty 81 86
 undo shell
 flow-control none
 redirect enable
#
```

（2）检查被管理设备 Console 口

DMC 设备如果无法正确识别设备，首先使用 PC 通过 Console 线缆连接被管理设备 Console 口，查看是否能正确进入设备控制台。

（3）排查线缆线序

DMC 服务器和成员设备之间的连接线缆线序如图 2-2 所示。

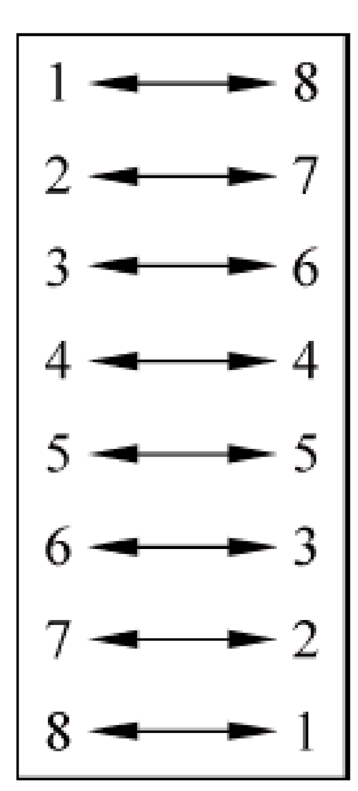


图 2-2　连接线缆线序

（4）检查串口板卡

若成员设备和线缆都已经确定没有问题，接下来可以排查 DMC 设备板卡，可以通过检查接口下是否有错包、更换 DMC 板卡槽位、更换能正常使用的其他正常板卡做替换测试从而确定板卡是否有问题。

命令：*display interface Async interface-number*

例如：通过命令查看路由器 Async 5/0 接口。

```
[DMC]display interface Async 5/0
Async5/0 current state: Up
Line protocol current state: Up
Description: Async5/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Last 300 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Input: 1 packets, 0 bytes
           0 broadcasts, 0 multicasts
           1 errors, 0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           1 frame errors
    Output:10 packets, 42 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
    DCD=Down  DTR=Up  DSR=Up  RTS=Up  CTS=Down
```

（5）查看被管理设备使用的软件版本

如果经过排查，上述步骤都没有问题，在 DMC 设备上使用反向 Telnet，确认是否能正常登录到被管理设备，如果反向 Telnet 能正常登录，但是 Web 页面无法正常使用，则进一步检查被管理设备的软件版本。

命令：*display version*

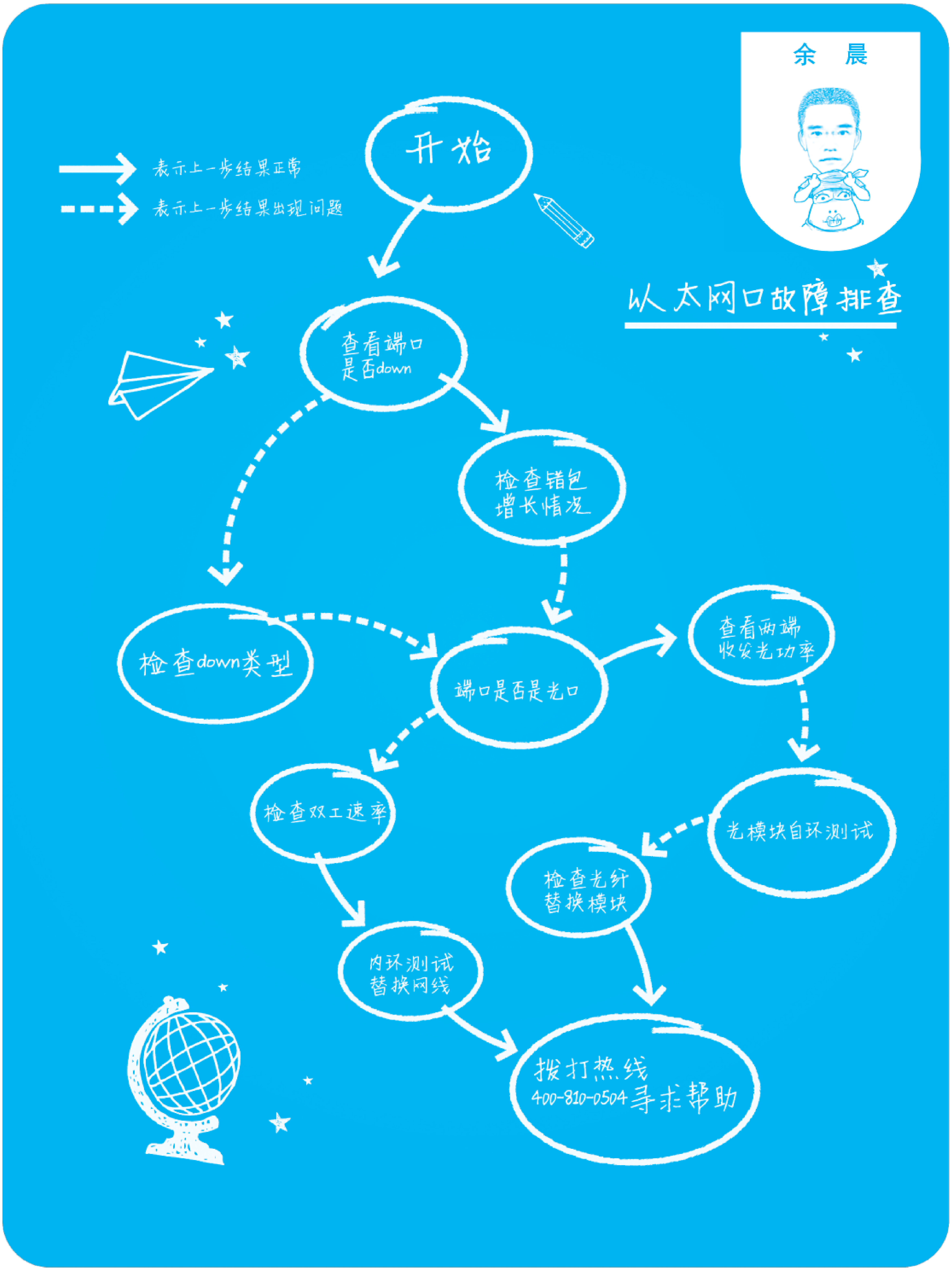
例如：通过命令查看被管理设备的软件版本。

```
[H3C] display version

H3C Comware Platform Software
Comware Software, Version 5.20, Release 2312P20, Standard
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR30-40 uptime is 0 week, 0 day, 0 hour, 14 minutes
Last reboot 2013/04/20 17:13:30
System returned to ROM By <Reboot> Command.
```

03

交换技术


余 晨
从太网口故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看端口是否down
检查错包增长情况
检查down类型
端口是否是光口
查看两端收发光功率
检查双工速率
光模块自环测试
检查光纤替换模块
内环测试替换网线
拨打热线 400-810-0504 寻求帮助

1．开始

以太网口定位故障的思路是：先查看端口状态，Up 时检查端口错包是否增长，根据错包类型排查链路，Down 时排查配置和链路，如果是电口检查协商状态，并进行内环测试，若是光口查看收发光功率是否正常，尾纤自环是否 Up，最后进行替换操作。

2．流程图相关操作说明

（1）查看端口是否 Down

查看物理端口状态，确认端口 Up。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令确认物理端口是否 Up。

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Down
…
```

（2）检查 Down 类型

查看物理端口状态，通常有 Up、物理 Down、Down(类型)三种状态。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，G1/0/1 为 Down（Administratively）状态，即端口视图下配置了 Shutdown。

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state:Down ( Administratively )
…
```

状态 Down 还有其他类型，如下。

① Link-Aggregation interface Down：聚合逻辑口配置 Shutdown。

② Loop Down：Loopback-Detection 监测到环路，端口被强制关闭。

③ BPDU-Protected：该端口在 BPDU Guard 功能的作用下被关闭。

④ Monitor-Link Uplink Down：同一个 Monitor Link 组里的上行端口 Down 导致本端口 Down。

⑤ Port Security Disabled：检测到端口收到非法报文，端口安全的入侵检测机制将端口关闭。

（3）检查错包增长情况

检查接口输入/输出是否有大量的错误包，如有则优化网络或排查链路。

命令：*display interface GigabitEthernet interface-number*

例如：查询端口 G1/0/2 端口信息，可以通过命令 *reset counters interface* 清除原有计数。

入方向：如果端口入包统计不增加，建议排查对端设备；如果端口入包的错误统计频繁增加：建议测试链路，替换网线或测试光衰，调整两端端口的工作模式。

出方向：查询对端的入包统计，如果 overruns、ignored 计数增加，建议排查对端设备，如果 CRC、frame、throttles 计数增加，建议替换链路，链路质量差或者线路光衰大会导致报文在

传输过程中出错。

```
<H3C>display interface GigabitEthernet 1/0/2
 GigabitEthernet1/0/2 current state: Down ( Link-Aggregation interface down )
 …
 Input (total):  4083 packets, 595822 bytes
         1785 unicasts, 501 broadcasts, 1797 multicasts, 0 pauses
 Input (normal):  4083 packets, - bytes
         1785 unicasts, 501 broadcasts, 1797 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total): 4198 packets, 593898 bytes
         1864 unicasts, 538 broadcasts, 1796 multicasts, 0 pauses
 Output (normal): 4198 packets, - bytes
         1864 unicasts, 538 broadcasts, 1796 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

（4）端口是否是光口

通过查看以太网端口类型。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，若显示 Media type is twisted pair 表示是双绞线作为媒介的电口，若显示 Media type is not sure，Port hardware type is No connector 一般认为是光口。

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Down ( Administratively )
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e2b2-35ae
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
Media type is not sure, Port hardware type is No connector
…
```

（5）检查双工速率

当设置端口为自协商（Auto）状态时，端口的速率双工状态由本端口和对端端口自动协商而定，两端双工速率需匹配一致。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，G1/0/1 自协商为千兆双工模式。

```
<H3C>display interface GigabitEthernet 1/0/1
 …
 Port hardware type is  1000_BASE_T
 1000Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 …
```

（6）内环测试替换网线

内环测试在交换芯片内部建立自环，用以确认接口内部没问题。

命令：*loopback internal*

例如：G1/0/1 自环测试成功。说明接口内部没问题，则可以通过替换网线排除物理链路故障，一般采用 5 类及 5 类以上双绞线。

```
[H3C-GigabitEthernet1/0/1]loopback internal
%Apr 26 12:08:44:576 2000 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Up.
 Loop internal succeeded!
%Apr 26 12:08:44:754 2000 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Down.
```

(7) 查看两端收发光功率

查看可插拔接口模块的数字诊断参数的当前测量值。

命令：*display transceiver diagnosis interface GigabitEthernet interface-number*

例如：查看 G1/1/1 的收发光功率，确保在正常范围内，接收到的功率应在接收灵敏度与过载功率之间，小于接收灵敏度接口不能 Up，大于过载功率可能已经造成模块损坏了。

```
[H3C]display transceiver diagnosis interface GigabitEthernet 1/1/1
GigabitEthernet1/1/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(℃)  Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    43        3.32        9.57      -3.77          -5.43
```

(8) 光模块自环测试

多模模块或 10km 单模模块，可以直接自环，用一根尾纤将光模块的 Rx 和 Tx 连接起来，确认接口是否可以 Up，如果可以 Up，说明本端光模块没有问题；否则，可能光模块有故障。

说明：

① 10km 以上的光模块不能直接自环，必须加光衰减器，必须保证接收光功率在正常范围内；

② 为避免该测试造成网络环路，需预先将端口加入非业务 VLAN。

(9) 检查光纤替换模块

检查光纤连接，通过替换光纤、模块排除物理链路故障。

命令：*display transceiver interface GigabitEthernet interface-number*

例如：通过命令分别显示 G1/1/1 接口模块的主要特征参数。分别表示模块类型、连接器类型、中心波长、传输距离、数字诊断功能、厂商名称、模块名称。确认选择适配的电缆、模块及光纤。

```
[H3C]display transceiver interface GigabitEthernet 1/1/1
GigabitEthernet1/1/1 transceiver information:
  Transceiver Type              : 1000_BASE_SX_SFP
  Connector Type                : LC
  Wavelength(nm)                : 850
  Transfer Distance(m)          : 550(50um),270(62.5um)
  Digital Diagnostic Monitoring : YES
  Vendor Name                   :H3C
  Ordering Name                 :SFP-GE-SX-MM850
```


余 晨
表示上一步结果正常
表示上一步结果出现问题
开始
以太网链路聚合故障排查
查看聚合端口状态
查看成员端口物理状态
检查成员端口数量
检查物理链路
检查本端及对端成员端口配置
查看是否动态聚合
检查成员端口Outbound流量
调整负载分担类型
检查端口收发LACP数量
检查本端成员端口配置
拨打热线400-810-0504寻求帮助

1．开始

链路聚合定位故障的思路是：先查聚合端口状态、聚合正常查看负载是否均衡，聚合异常先排查物理链路及成员端口数是否超规格，再根据聚合类型检查本端配置及对端配置，动态聚合可以检查端口 LACP 报文收发数量。

2．流程图相关操作说明

(1) 查看聚合端口状态

查看链路聚合组状态。

命令：*display link-aggregation summary*

display link-aggregation verbose

例如：通过命令确认二层链路聚合组 BAGG1 选中端口为 2 个。成员端口分别为 GE1/0/1、GE1/0/2。

```
<H3C>display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0023-893b-7085

AGG        AGG     Partner ID              Select Unselect   Share
Interface  Mode    Ports                   Ports             Type
--------------------------------------------------------------------------
BAGG1      S       none                    2        0        Shar
BAGG2      D       0x8000, 0023-896a-208a  2        0        Shar

[H3C]display link-aggregation verbose
…
Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port            Status  Priority  Oper-Key
--------------------------------------------------------------------------
  GE1/0/1         S       32768     1
  GE1/0/2         S       32768     1
…
```

(2) 检查成员端口 Outbound 流量

检查本端负载是否均衡，需检查本端聚合组内成员端口的出方向流量或对端入方向流量。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令显示聚合组成员端口 G1/0/1 的出方向流量，与 G1/0/2 进行比较确认负载是否均衡。

```
[H3C]display interface GigabitEthernet 1/0/1
...
Last 300 seconds input:   0 packets/sec 38 bytes/sec 0%
 Last 300 seconds output:   0 packets/sec 41 bytes/sec 0%
 Input (total):   49 packets, 11629 bytes
          5 unicasts, 25 broadcasts, 19 multicasts, 0 pauses
 Input (normal):   49 packets, - bytes
          5 unicasts, 25 broadcasts, 19 multicasts, 0 pauses
 Input:   0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 53 packets, 12536 bytes
       7 unicasts, 12 broadcasts, 34 multicasts, 0 pauses
 Output (normal): 53 packets, - bytes
          7 unicasts, 12 broadcasts, 34 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

(3) 调整负载分担类型

检查全局采用的聚合负载分担类型,可以通过如下命令查看。配置聚合负载分担类型时有可能出现丢包现象,尽量在无业务时调整。

命令:*display link-aggregation load-sharing mode*

例如:通过命令确认二层报文根据源/目的 MAC 地址及报文入端口进行聚合负载分担,三层报文根据源/目的 IP 地址进行聚合负载分担。在系统视图下进行全局聚合负载分担类型配置,根据报文类型、源 IP、目的 IP、源 MAC、目的 MAC、源端口、目的端口等不同的组合进行聚合负载分担。

```
[H3C]display link-aggregation load-sharing mode
Link-AggregationLoad-Sharing Mode:
Layer 2 traffic: ingress-port,              destination-mac address,
                 source-mac address
Layer 3 traffic: destination-ip address,    source-ip address
```

(4) 查看成员端口物理状态

查看物理端口状态,确认端口是否 Up。

命令:*display interface GigabitEthernet interface-number*

例如:通过命令确认物理端口是否 Up。

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
...
```

(5) 检查物理链路

当端口物理状态不 Up 时,根据端口类型查自协商、光功率,替换端口、网线、光纤模块。参考以太网口故障排查。

(6) 检查成员端口数量

检查链路聚合组成员端口数量,可通过端口替换操作排查可聚合端口数目是否超限制。

命令:*display link-aggregation summary*

例如：查看BAGG3选中端口数为8，未选中端口为1。断开任一选中端口，未选中端口即变为选中状态，避免业务运行时调整成员端口数量。

```
<H3C>display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode:S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0023-893b-7085

AGG         AGG        Partner ID              Select Unselect  Share
Interface   Mode                               Ports  Ports     Type
-------------------------------------------------------------------
BAGG3       S          none                    8      1         Shar
```

(7) 查看是否动态聚合

查看链路聚合组类型。

命令：*display link-aggregation summary*

例如：通过命令查看二层链路聚合组BAGG1为静态聚合，BAGG2为动态聚合。

```
<H3C>display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 0023-893b-7085

AGG         AGG        Partner ID              Select Unselect  Share
Interface   Mode                               Ports  Ports     Type
-------------------------------------------------------------------
BAGG1       S          none                    2      0         Shar
BAGG2       D          0x8000, 0023-896a-208a  2      0         Shar
```

(8) 检查本端及对端成员端口配置

检查本端物理接口与对端物理口配置是否一致，检查物理口与逻辑口配置是否一致。

命令：*display current-configuration interface interface-number*

例如：通过命令确认本端选中端口g1/0/3和g1/0/4配置一致，并与对端保持一致。

```
[H3C]display current-configuration interface g1/0/3
#
interface GigabitEthernet1/0/3
port link-mode bridge
 port link-aggregationgroup 2
#
return
[H3C]display current-configuration interface g1/0/4
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-aggregation group 2
```

（9）检查端口收发 LACP 数量

检查本端口和对端端口 LACP 报文收发数量。

命令：*display link-aggregation member-port*

例如：通过命令显示检查聚合成员端口 LACP 数量是否增长。通过 reset lacp statistics 清除所有成员端口上的 LACP 统计信息。

```
[H3C]display link-aggregation member-port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
GigabitEthernet1/0/3:
Aggregation Interface: Bridge-Aggregation2
…
Received LACP Packets:18 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets:41 packet(s)

GigabitEthernet1/0/4:
Aggregation Interface: Bridge-Aggregation2
…
Received LACP Packets:17 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets:43 packet(s)
```

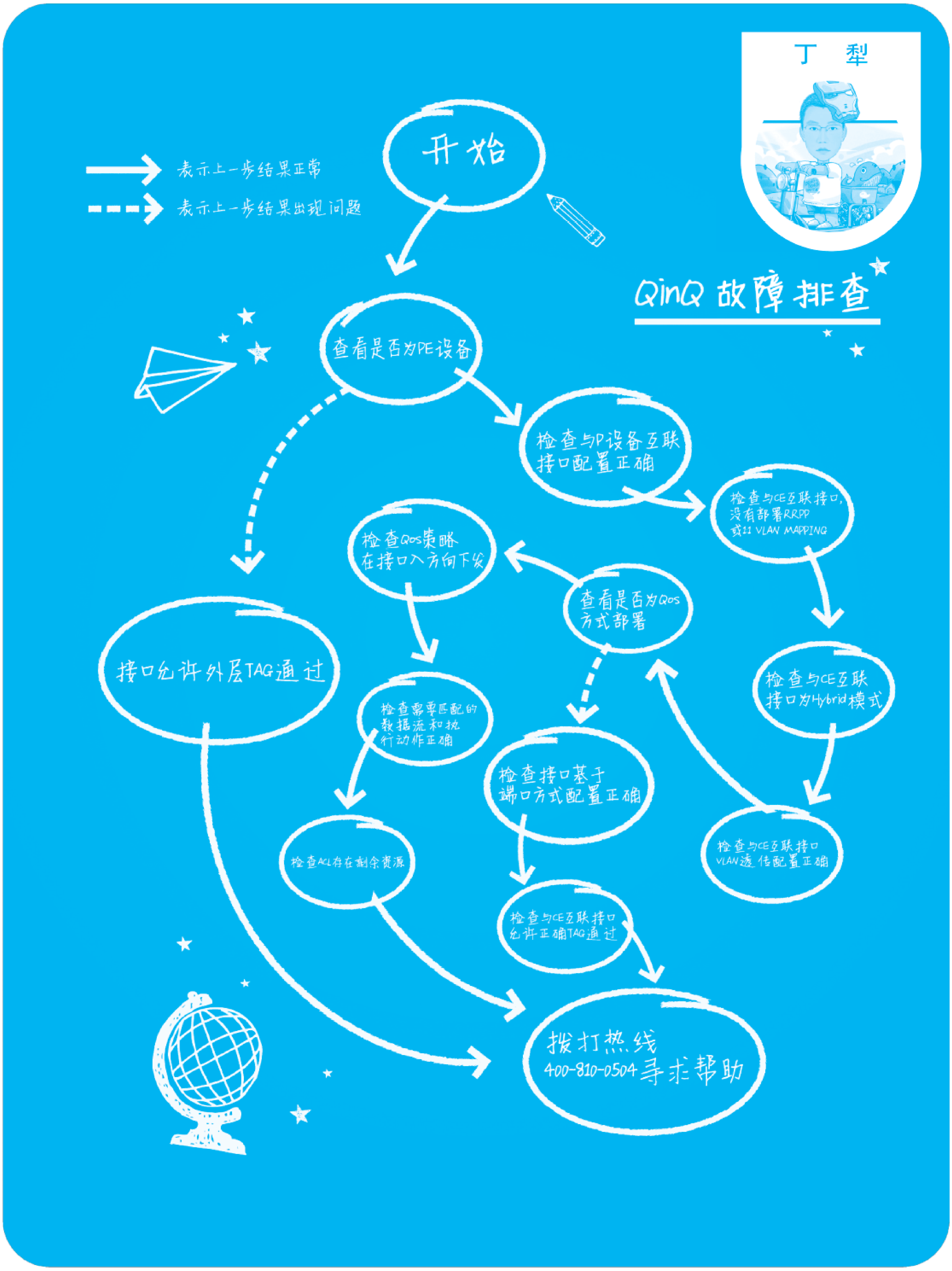
（10）检查本端成员端口配置

静态聚合时，务必保证各物理端口配置一致，且物理端口与聚合逻辑口配置一致。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令显示检查链路聚合组逻辑口和聚合组的配置，确认保持一致。

```
<H3C>display current-configuration interface Bridge-Aggregation 1
#
interface Bridge-Aggregation1
#
return
<H3C>display current-configuration interface GigabitEthernet 1/0/1
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-aggregation group 1
#
<H3C>display current-configuration interface GigabitEthernet 1/0/2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-aggregation group 1
#
```


丁 犁
QinQ 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看是否为PE设备
检查与P设备互联接口配置正确
检查与CE互联接口，没有部署RRPP或1:1 VLAN MAPPING
检查与CE互联接口为Hybrid模式
检查与CE互联接口VLAN透传配置正确
查看是否为QoS方式部署
检查QoS策略在接口入方向下发
检查需要匹配的数据流和执行动作正确
检查ACL存在剩余资源
检查接口基于端口方式配置正确
检查与CE互联接口允许正确TAG通过
接口允许外层TAG通过
拨打热线400-810-0504寻求帮助

1. 开始

定位故障的思路是：如果是P设备，确保接口允许外层TAG通过。如果是PE设备，首先检查接口类型是否符合要求，再检查设备是否满足QinQ部署要求，最后检查设备硬件资源是否足够。

2. QinQ排错相关操作说明

(1) 查看是否为PE设备

QinQ网络部署分为P设备和PE设备，请根据设备部署类型，选择对应的排查方向。

(2) 接口允许外层TAG通过

命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，GE2/0/10接口允许外层Tag 100通过。

```
<H3C>display interface GigabitEthernet 2/0/10
…
PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 100, 200
  Trunk port encapsulation: IEEE 802.1q
…
```

(3) 检查与P设备互联接口配置正确

① 检查与P设备互联接口允许外层Tag通过。

命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，GE2/0/10接口是否允许外层Tag 100通过。

```
<H3C>display interface GigabitEthernet 2/0/10
…
PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 100, 200
  Trunk port encapsulation: IEEE 802.1q
…
```

② 检查与P设备互联接口TPID值配置正确。两端设备交互报文中，若TPID不一致，报文将无法互通。默认H3C设备为8100。

例如：检查与P设备互联端口2/0/10 VLAN Tag的TPID值是否匹配。

说明：Qos方式在接口模式下修改TPID，不同接口TPID可不同；基于端口方式在配置模式下修改TPID，整机TPID保持一致。

```
Qos 方式:
[H3C-GigabitEthernet2/0/10]display this
#
 interface GigabitEthernet2/0/10
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 qinq ethernet-type service-tag 8200
#
基于端口方式:
[H3C]display this
...
[H3C] qinq  ethernet-type service-tag 8300
...
```

(4) 检查与 CE 互联接口,没有部署 RRPP 或 1∶1 VLAN MAPPING

QinQ 端口不使能 RRPP 功能和 1∶1 VLAN Mapping 功能。

(5) 检查与 CE 互联接口为 Hybrid 模式

查看设备接口类型为 Hybrid 模式,允许相应 Tag 通过。

命令: *display port hybrid*

例如: 通过命令查看,确认设备与 CE 互联 GE2/0/1 端口模式为 Hybrid,且允许用户 VLAN10 报文被封装为 VLAN 100 后在网络中传递。

```
Qos 方式:
<H3C>display port hybrid
Interface                 PVID        VLAN passing
GE2/0/1                   1           Tagged:   none
                                      Untagged:1, 100,
基于端口方式:
<H3C>display port hybrid
Interface                 PVID        VLAN passing
GE2/0/1                   1           Tagged:   10,
                                      Untagged:100,
```

(6) 检查与 CE 互联接口 VLAN 透传配置正确

检查需要进行 QinQ 封装的用户 VLAN 不在透传范围内。

例如: 查看 GE2/0/1 接口配置,VLAN90 至 VLAN99 为需要透传的 VLAN,QinQ 用户 VLAN10 封装外层 Tag 不在透传范围内,命令为 *display current-configuration interface GigabitEthernet interface-number*

```
<H3C>display current-configuration interface GigabitEthernet 2/0/1
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 100 untagged
 qinq enable
 qinq transparent-vlan 90 to 99
 qos apply policy qinq inbound
#
```

（7）查看是否为 Qos 方式部署

与 CE 互联的接口部署 QinQ 时，有两种方式。一种为 Qos 方式部署；另一种为基于端口方式部署。请根据不同部署方式，选择对应的排查方向。

（8）检查接口基于端口方式配置正确

命令：*display current-configuration interface GigabitEthernet interface-number*

例如：确认在设备 GE2/0/1 接口将 VLAN10 报文封装为 LAN100。

```
<H3C>display current-configuration interface GigabitEthernet 2/0/1
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 tagged
 port hybrid vlan 100 untagged
 qinq enable
 qinq vid 100
 raw-vlan-id inbound 10
#
```

如果配置时出现以下报错，表示设备资源不足，需调整配置。

Error：Not enough resource on interface GigabitEthernet 1/0/10

（9）检查与 CE 互联接口允许正确 Tag 通过

命令：*display current-configuration interface GigabitEthernet interface-number*

例如：通过命令查看，确认设备 GE2/0/1 端口允许 VLAN10 报文带 Tag 通过，允许 VLAN100 报文不带 Tag 通过。

```
<H3C>display current-configuration interface GigabitEthernet 2/0/1
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 tagged
 port hybrid vlan 100 untagged
 qinq enable
 qinq vid 100
 raw-vlan-id inbound 10
#
```

（10）检查 Qos 策略在接口入方向下发

采用 Qos 方式部署 QinQ，需要在用户互联端口 Inbound 方向下发。

命令：*display qos policy interface GigabitEthernet interface-number*

例如：通过命令查看，确认 Qos 在设备 GE2/0/1 端口 Inbound 方向下发。

```
<H3C>display qos policy interface GigabitEthernet 2/0/1
  Interface: GigabitEthernet2/0/1
  Direction: Inbound
  Policy: qinq
  Classifier: qinq
```

```
    Operator: AND
    Rule(s) : If-match customer-vlan-id 10
    Behavior: qinq
    Nesting: Nest top-most vlan-id 100
```

(11) 检查需要匹配的数据流和执行动作正确

命令：*display qos policy interface GigabitEthernet interface-number*

例如：通过命令查看设备 GE2/0/1 端口，匹配用户 VLAN10；对匹配的 VLAN 执行封装外层 Tag 100 的动作。

```
<H3C>display qos policy interface GigabitEthernet 2/0/1
  Interface: GigabitEthernet2/0/1
  Direction: Inbound
  Policy: qinq
  Classifier: qinq
  Operator: AND
  Rule(s) :If-match customer-vlan-id 10
  Behavior: qinq
  Nesting: Nest top-most vlan-id 100
```

(12) 检查 ACL 存在剩余资源

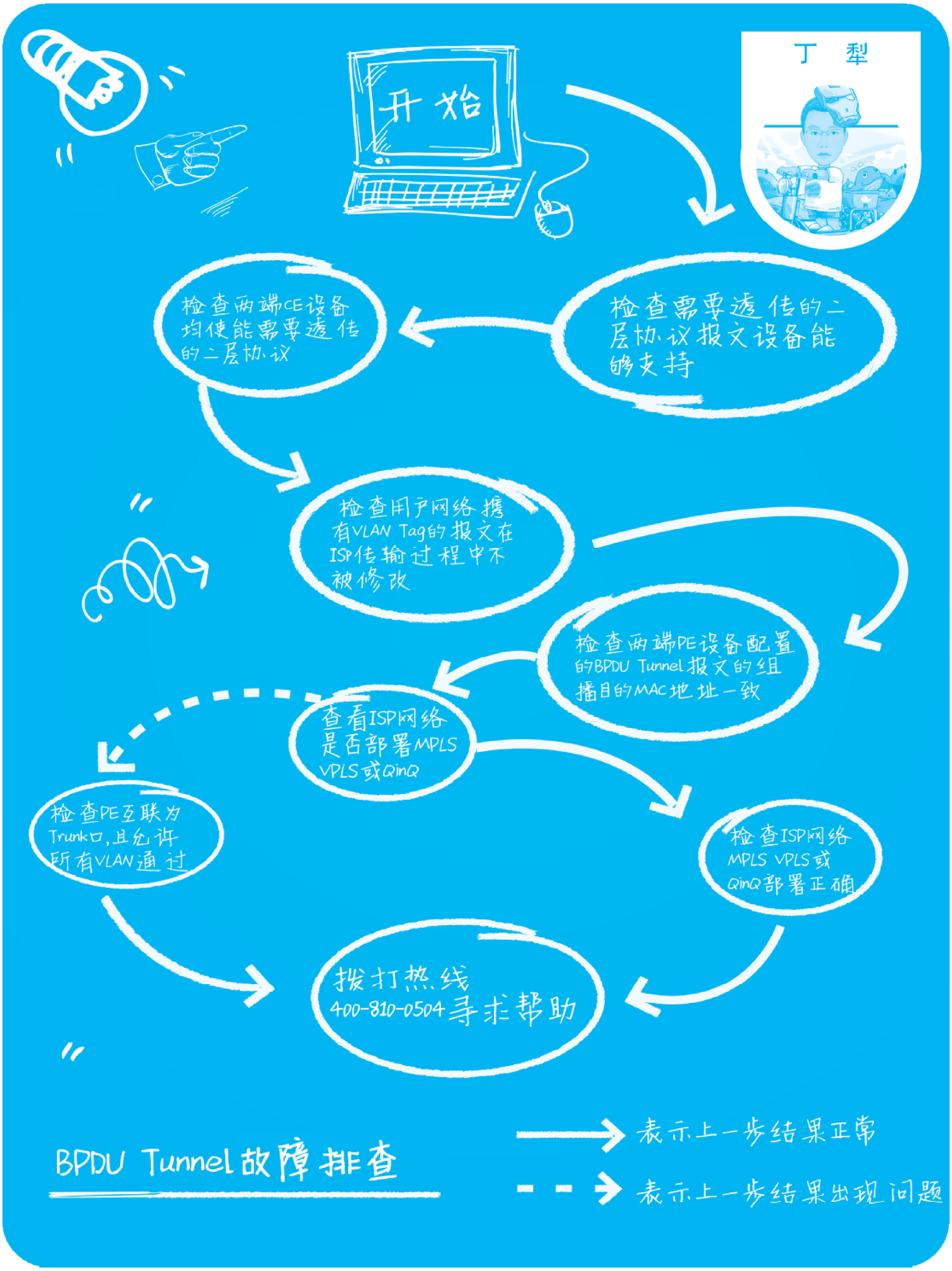
设备资源不足将导致 QinQ 无法部署。

使用 Qos 方式部署时将占用 ACL 资源，需检查 ACL 资源是否剩余。

命令：*display acl resource*

例如：Qos 方式部署时，通过命令查看设备 ACL VFP 资源剩余 1535 条资源。

```
<H3C>display acl resource
 Interface:
   GE1/0/1 to GE1/0/24, XGE1/1/1 to XGE1/1/2
----------------------------------------------------------------------
 Type          Total     Reserved    Configured   Remaining    Usage
----------------------------------------------------------------------
 VFP ACL       2048      512         1            1535         25%
 IFP ACL       8192      2048        0            6144         25%
 IFP Meter     4096      1024        0            3072         25%
 IFP Counter   4096      1024        0            3072         25%
 EFP ACL       1024      0           0            1024         0%
 EFP Meter     512       0           0            512          0%
 EFP Counter   512       0           0            512          0%
```



丁 犁
开始
检查需要透传的二层协议报文设备能够支持
检查两端CE设备均使能需要透传的二层协议
检查用户网络携有VLAN Tag的报文在ISP传输过程中不被修改
检查两端PE设备配置的BPDU Tunnel报文的组播目的MAC地址一致
查看ISP网络是否部署MPLS VPLS或QinQ
检查PE互联为Trunk口，且允许所有VLAN通过
检查ISP网络MPLS VPLS或QinQ部署正确
拨打热线400-810-0504寻求帮助
BPDU Tunnel故障排查
表示上一步结果正常
表示上一步结果出现问题

1. 开始

定位故障的思路是：首先检查两端 CE 设备均使能了需要透传的二层协议，再检查两端 PE 设备配置的 BPDU Tunnel 报文的组播目的 MAC 地址一致，最后根据 ISP 网络类型检查相关配置是否正确。

2. BPDU Tunnel 排错相关操作说明

(1) 查看检查需要透传的二层协议报文设备能够支持

H3C 设备支持以下协议的 BPDU Tunnel 功能。

```
CDP(Cisco Discovery Protocol,思科发现协议)
DLDP(Device Link Detection Protocol,设备链路检测协议)
EOAM(Ethernet Operation, Administration and Maintenance,以太网操作、管理和维护)
GVRP(GARP VLAN Registration Protocol,GARP VLAN 注册协议)
HGMP(HW Group Management Protocol,HW 组管理协议)
LACP(Link Aggregation Control Protocol,链路聚合控制协议)
LLDP(Link Layer Discovery Protocol,链路层发现协议)
PAgP(Port Aggregation Protocol,端口聚合协议)
PVST(Per VLAN Spanning Tree,每 VLAN 生成树)
STP(Spanning Tree Protocol,生成树协议)
UDLD(Uni-Directional Link Direction,单向链路检测)
VTP(VLAN Trunking Protocol,VLAN 中继协议)
```

(2) 接检查两端 CE 设备均使能需要透传的二层协议

两端 CE 均需要使能需要透传的二层协议，以保证二层协议报文在传递后，对端 CE 能够正常处理。

例如：通过命令查看，两端 CE 设备使能 STP 协议。

```
<CE1>display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID             : 32768.0cda-41b4-e62c
 Bridge times          : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
…
<CE2>display stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID             : 32768.0cda-414c-e32c
 Bridge times          : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
…
```

(3) 检查用户网络携有 VLAN Tag 的报文在 ISP 传输过程中不被修改

通过抓包，确认用户网络协议报文中携带的二层 VLAN Tag 部分不被修改。

(4) 检查两端 PE 设备配置的 BPDU Tunnel 报文的组播目的 MAC 地址一致

检查两端 PE 设备配置的 BPDU Tunnel 报文的组播目的 MAC 地址一致，且组播目的 MAC 地址符合设备要求。

命令：*bpdu-tunnel tunnel-dmal mac-address*

```
BPDU Tunnel 报文默认采用的组播目的 MAC 地址为 010F-E200-0003。
用户可以根据需要将其修改为 0100-0CCD-CDD0、0100-0CCD-CDD1 或 0100-0CCD-CDD2 地址。

在两端 PE 上检查配置的组播 MAC 地址一致
[PE1] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
[PE2] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

(5) 查看 ISP 网络是否部署 MPLS、VPLS 或 QinQ

ISP 网络有多种部署方式。一种为 MPLS、VPLS 或 QinQ 方式部署；另一种为基本网络方式部署。请根据不同部署方式，选择对应的排查方向。

(6) 检查 PE 互联为 Trunk 口，且允许所有 VLAN 通过

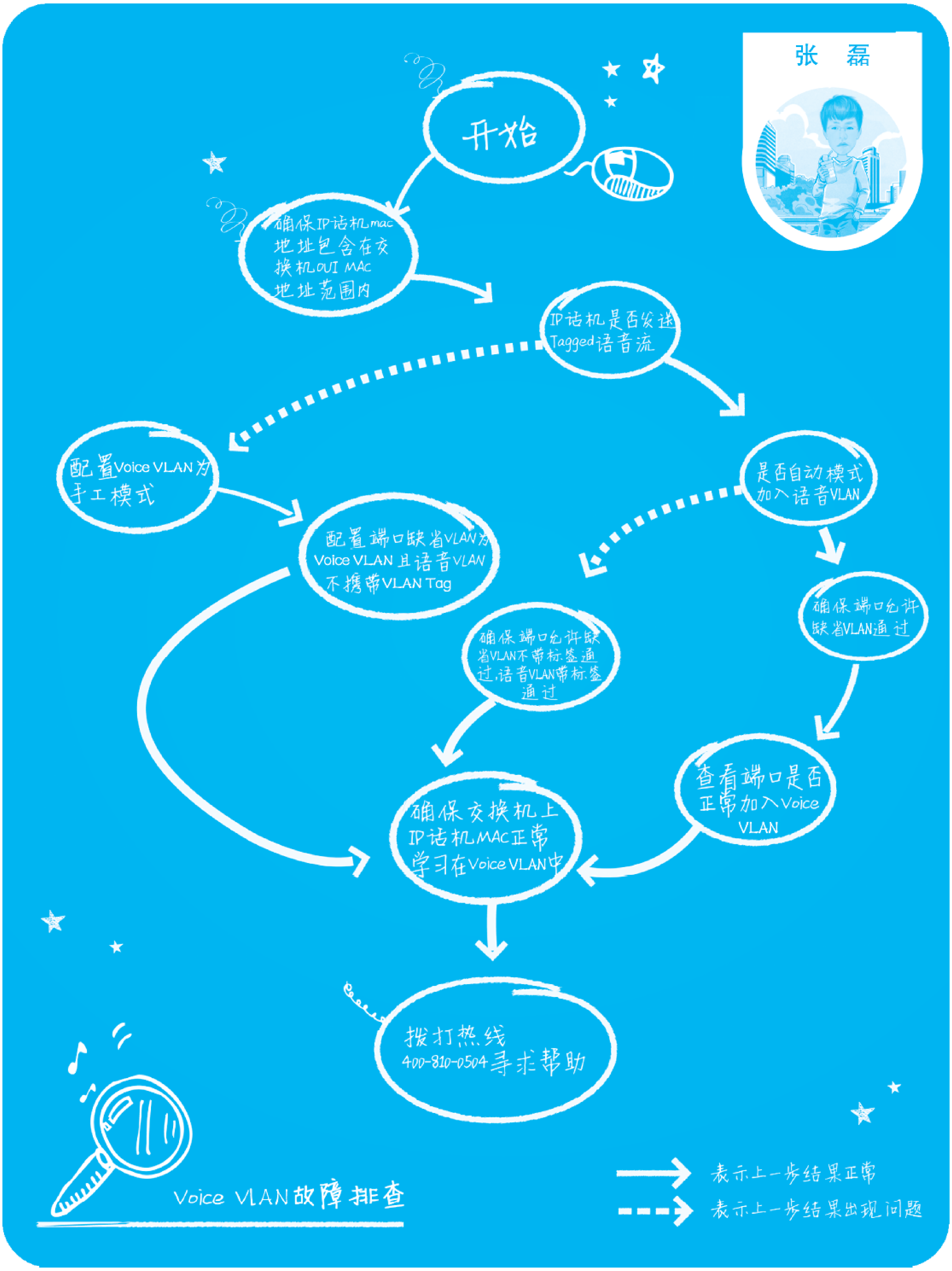
命令：*display interface GigabitEthernet interface-number*

例如：通过命令查看，GE1/0/10 PE 互联接口为 Trunk 类型，且允许所有 VLAN 通过。

```
<PE1>display interface GigabitEthernet 1/0/10
...
PVID: 1
 Mdi type: auto
 Port link-type:trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 2-4094
  Trunk port encapsulation: IEEE 802.1q
...
```

(7) 检查 ISP 网络 MPLS、VPLS 或 QinQ 部署正确

具体检查方法，请查阅相关协议故障排查方式。


张 磊
开始
确保IP话机mac地址包含在交换机OUI MAC地址范围内
IP话机是否发送Tagged语音流
配置Voice VLAN为手工模式
是否自动模式加入语音VLAN
配置端口缺省VLAN为Voice VLAN且语音VLAN不携带VLAN Tag
确保端口允许缺省VLAN通过
确保端口允许缺省VLAN不带标签通过,语音VLAN带标签通过
查看端口是否正常加入Voice VLAN
确保交换机上IP话机MAC正常学习在Voice VLAN中
拨打热线 400-810-0504寻求帮助
Voice VLAN故障排查
表示上一步结果正常
表示上一步结果出现问题

1. 开始

定位故障的思路是：首先确保 IP 话机 MAC 地址包含在交换机 OUI MAC 地址范围内，根据 IP 话机发送的语音报文是否携带 Tag 来检查相关配置信息，最后查看端口是否正常加入 Voice VLAN，查看 IP 话机 MAC 地址是否学习在正常的 Voice VLAN 中。

2. 流程图相关操作说明

(1) 确保 IP 话机 MAC 地址包含在交换机 OUI MAC 地址范围内

通过命令行可以查看交换机上配置的 OUI MAC 地址范围。

命令：*display voice vlan oui*

例如：通过命令查看，可以确认目前交换机上存在 6 个段的 OUI MAC 地址范围。

```
<H3C> display voice vlan oui
Oui Address      Mask             Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
0011-1100-0000   ffff-ff00-0000   IP phone A
0011-2200-0000   ffff-ff00-0000   IP phone B
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3com phone
```

(2) IP 话机是否发送 tagged 语音流

目前 IP 话机可以发送 tagged 及 untagged 语音流，IP 话机一般可以通过 dhcp 获取或者手工指定的方式确定语音报文携带的 VLAN 号或者语音报文已 untagged 的方式发送。

(3) 配置 Voice VLAN 为手工模式

通过以下命令设置交换机端口的工作模式为手工模式。

命令：*undo voice vlan mode auto*

例如：通过以下的命令设置端口 GigabitEthernet1/0/1 工作在手动模式。

```
[H3C] interface gigabitethernet 1/0/1
[H3C-GigabitEthernet1/0/1] undo voice vlan mode auto
```

(4) 配置端口默认 VLAN 为 Voice VLAN 且语音 VLAN 不携带 VLAN Tag

对于 Acess 类型端口直接加入 Voice VLAN 即可。

对于 Trunk 类型的端口配置配置 pvid 为 Voice VLAN。

对于 Hybrid 类型端口配置 pvid 为 Voice VLAN 且 Voice VLAN untagged 通过。

(5) 是否自动加语音 VLAN

通过以下命令设置交换机端口的工作模式为自动模式。

命令：*voice vlan mode auto*

例如：通过以下的命令设置端口 GigabitEthernet1/0/1 工作在自动模式。

```
[H3C] interface gigabitethernet 1/0/1
[H3C-GigabitEthernet1/0/1]voice vlan mode auto
```

(6) 确保端口允许默认 VLAN 不带标签通过,语音 VLAN 带标签通过

对于 Acess 类型端口不支持 IP 话机发送 Tagged 类型的语音报文。

对于 Trunk 类型的端口配置配置 pvid 为非 Voice VLAN 且允许 pvid VLAN 通过,配置语音 VLAN 通过。

对于 Hybrid 类型端口配置 pvid 为非 Voice VLAN 且允许 pvid VLAN untagged 通过。配置 Voice VLAN tagged 通过。

(7) 确保端口允许默认 VLAN 通过

对于 Acess 类型端口不支持 IP 话机发送 Tagged 类型的语音报文。

对于 Trunk 类型的端口配置配置 pvid 为非 Voice VLAN 且允许 pvid VLAN 通过。

对于 Hybrid 类型端口配置 pvid 为非 Voice VLAN 且允许 pvid VLAN untagged 通过。

(8) 查看端口是否正常加入 Voice VLAN

自动模式情况下端口会自动加入语音 Voice VLAN,可以通过命令行查看端口下是否允许了语音 VLAN 通过。

命令:*display interface interface-type interface-number*

通过以下命令可以看到端口 5/0/3 端口允许了 2、3、101 这三个 VLAN 通过。

```
<H3C> display interface GigabitEthernet5/0/3
GigabitEthernet5/0/3 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8928-f1dd
 Description: ** connect to LC-Sw-H3652
 Loopback is not set
 Media type is optical fiber,Port hardware type is 1000_BASE_SX_SFP
 1000Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: trunk
 VLAN passing   : 2-3, 101
  VLAN permitted: 2-4094
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
 Last clearing of counters:   Never
 Peak value of input: 6 bytes/sec, at 2014-01-04 16:13:01
 Peak value of output: 3473 bytes/sec, at 2014-01-09 00:37:00
```

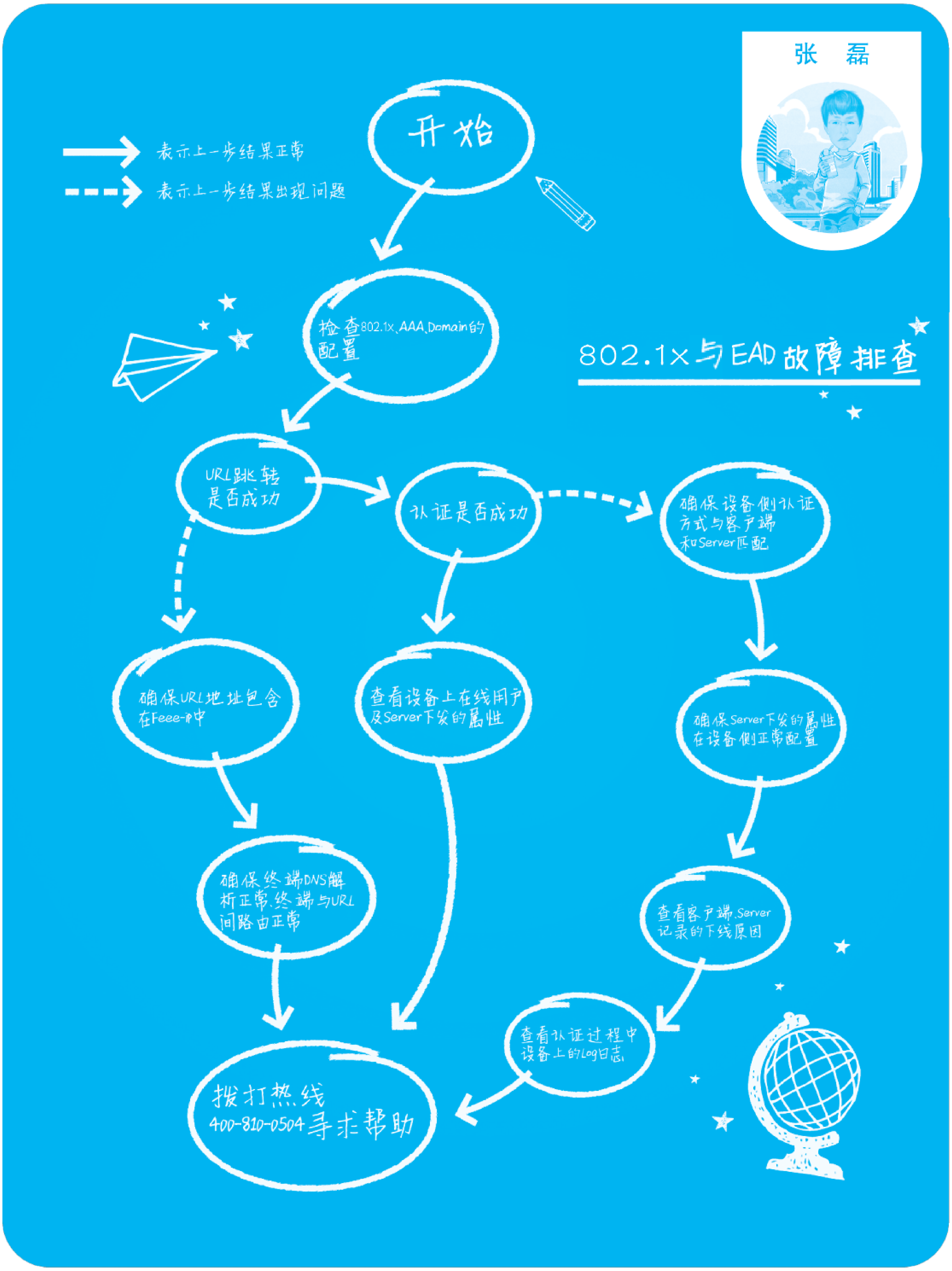
(9) 确保交换机上 IP 话机的 MAC 地址正常学习到 Voice VLAN 中

通过下面命令可以查看 MAC 地址学习情况。

命令：*display mac-address mac-address-number*

例如：通过下面的命令可以看到 000f-e201-0101 这个 MAC 地址在 VLAN 中。

```
#显示 MAC 地址表中 MAC 地址为 000f-e201-0101 的表项的信息。
<Sysname> display mac-address 000f-e201-0101
MAC ADDR         VLAN ID    STATE          PORT INDEX       AGING TIME(s)
000f-e201-0101   1          Learned        Ethernet1/0/1    AGING
  ---  1 mac address(es) found  ---
```


张 磊
802.1x与EAD故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查802.1x、AAA、Domain的配置
URL跳转是否成功
认证是否成功
确保设备侧认证方式与客户端和Server匹配
确保URL地址包含在Feee-ip中
查看设备上在线用户及Server下发的属性
确保Server下发的属性在设备侧正常配置
确保终端DNS解析正常，终端与URL间路由正常
查看客户端、Server记录的下线原因
查看认证过程中设备上的Log日志
拨打热线400-810-0504寻求帮助

1. 开始

定位故障的思路是：以 802.1x 认证流程为基本方向。排查设备的基本配置后，关于 URL 跳转部分，先查看终端是否可以正常跳转至 URL，然后确保 URL 包含在 Free-IP 中，确保终端与 URL 主机间的连通性正常。关于认证部分，首先确保设备上 802.1x 认证方式正确，然后查看设备侧是否手工配置 Radius Server 下发的相关属性，最后查看客户端、Radius Server 上记录的认证失败原因及查看设备的相关 Log。

2. 流程图相关操作说明

（1）检查 802.1x、AAA、Domain 的配置

检查 802.1x、AAA、Domain 等配置，各部分注意事项如下。

① 802.1x 部分。在全局配置及接口下使能 802.1x 认证。

例如：通过当前配置可确认在全局及接口 GigabitEthernet1/0/1 下使能了 802.1x。

```
#
 dot1x
#
 interface GigabitEthernet1/0/1
 port link-mode bridge
 dot1x
#
```

② AAA 部分。配置 Radius Scheme 认证方案，指定认证、计费服务器。配置 Nas-Ip 且保证 Nas-Ip 到认证、计费服务器可达。同时保证 User-Name-Format 和 Server-Type 与 Radius Server 匹配。

例如：通过当前配置可知 Radius Scheme 的 Server-Type 为 Extended，User-Name-Format 为 Without-Domain。认证计费 Server 都为 1.1.1.1。

```
#
radius scheme h3c
 server-type extended
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 key authentication cipher $c$3$hmc/dsendG8XM8FKqsWbR7wjO0vF4A==
 key accounting cipher $c$3$PXWZGLZ4d64iZDVzdWn5nL2yJrv/uA==
 user-name-format without-domain
#
```

③ Domain 部分。在 Domain 视图下引用相应的 Radius Scheme 方案，认证授权方案必须同时指定。

例如：通过当前配置可知，Domain 下引用的 Radius Scheme 方案为 H3C。

```
#
domain h3c
```

```
authentication lan-access radius-scheme h3c
authorization lan-access radius-scheme h3c
accounting lan-access radius-scheme h3c
access-limit disable
state active
idle-cut disable
self-service-url disable
#
```

（2）URL 跳转是否成功

在浏览器中访问任意网站，设备都会将其重定向至 URL 页面。

（3）确保 URL 地址包含在 Free-IP 中

在终端认证成功之前仅有 Free-Ip 中的地址才允许访问，因此需确保 URL 地址包含在 Free-Ip 中。

命令：*display dot.1x*

例如：通过命令查看，可以确认 URL 地址 6.6.6.6 包含在 Free-Ip 6.6.6.0/24 范围内。

```
<H3C>display dot.1x
 Equipment 802.1x protocol is enabled
 CHAP authentication is enabled
 EAD quick deploy is enabled

 Configuration: Transmit Period        30 s,  Handshake Period        15 s
                Quiet Period           60 s,  Quiet Period Timer is disabled
                Supp Timeout           30 s,  Server Timeout          100 s
                Reauth Period          3600 s
                The maximal retransmitting times     2
 EAD quick deploy configuration:
                URL: http://6.6.6.6:8080/ead
                Free IP:    6.6.6.0 255.255.255.0
                EAD timeout:   30 m
```

（4）确保终端 DNS 解析正常、终端与 URL 间路由正常

只有终端 DNS 解析正常、终端与 URL 间路由正常，URL 跳转才可以正常进行。

（5）认证是否成功

查看终端上返回的认证结果可以确认本次认证是否成功。

（6）查看设备上在线用户及 Server 下发的属性

通过下面的命令可以查看设备上的在线用户。

命令：*display connection*

例如：通过命令查看，可以确认此时设备上存在 H3C 用户在线，且其 index 为 1。

```
<H3C>display  connection
Slot:  1
Index=1    , Username=h3c@system
 IP=N/A
 IPv6=N/A
 MAC=60eb-6926-aca4
 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

通过下面的命令可以进一步确认特定用户的具体属性。

命令：*display connection ucibindex index*

例如：通过命令查看，可以确认 Server 向 h3c 用户下发了 VLAN 10，ACL 3000。

```
<H3C>display  connection ucibindex  1
Slot:  1
Index=1    , Username=h3c@system
MAC=60eb-6926-aca4
IP=N/A
IPv6=N/A
Access=802.1x    ,AuthMethod=CHAP
Port Type=Ethernet,Port Name=GigabitEthernet1/0/24
Initial VLAN=1,Authorization VLAN=10
ACL Group=3000
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A,   Terminate-Action=N/A
Start=2000-05-02 22:01:18 ,Current=2000-05-02 22:01:38 ,Online=00h00m20s
Total 1 connection matched.
```

（7）确保设备侧认证方式与客户端和 Server 匹配

确保设备侧 Authentication-Method 与客户端和 Server 匹配，例如，赛门铁克的客户端及 Server 要求设备的认证方法为 EAP。

命令：*display dot.1x*

例如：通过命令查看，设备目前配置的 802.1x 系统的认证方法为 EAP。

```
<H3C>display dot1x
 Equipment 802.1x protocol is enabled
 EAP authentication is enabled
 EAD quick deploy is enabled
 ...
```

（8）确保 Server 下发属性在设备侧正常配置

设备支持 Server 向其下发授权、隔离 VLAN，若设备侧接收到字符串形式的 VLAN Name 时，要求该 VLAN 必须是静态配置的，若收到整形的 VLAN ID 时，设备可以自动创建该 VLAN。

命令：*display vlan static*

例如：通过命令查看，设备上存在 VLAN 1、VLAN 2 两个静态 VLAN。

```
<H3C>display  vlan static
 Total 5 static VLAN exist(s).
 The following static VLANs exist:
  1(default), 2,
```

命令：*display vlan vlanid*

例如：通过命令查看，VLAN 3 的 Name 为 OA。

```
<H3C>display  vlan  3
 VLAN ID: 3
```

```
VLAN Type: static
Route Interface: configured
Description: VLAN 0003
Name:OA
Tagged   Ports: none
Untagged Ports: none
```

设备支持 Server 向其下发 ACL。向设备下发 ACL 时，设备上必须提前手工配置该 ACL。

命令：*display acl all*

例如：通过命令查看，设备上存在 ACL 3000。

```
<H3C>display acl all
Advanced ACL3000, named -none-, 2 rules,
 Geli acl
 ACL's

step is 5
 rule 0 permit ip destination 1.1.1.0 0.0.0.255
 rule 5 deny ip
```

(9) 查看客户端、Server 记录的下线原因

根据客户端及 Server 上常见的下线原因初步判断故障点。

例如，下线原因为 User Request，表示用户主动下线。如启用策略服务器的情况下，若 iNode 客户端与策略服务器通信的端口(UDP 9019)不通，iNode 会给出类似“未收到服务器回应，即将强行下线”的提示。

例如，图 3-1 是 iNode 客户端与策略服务器通信的端口不通导致的下线。

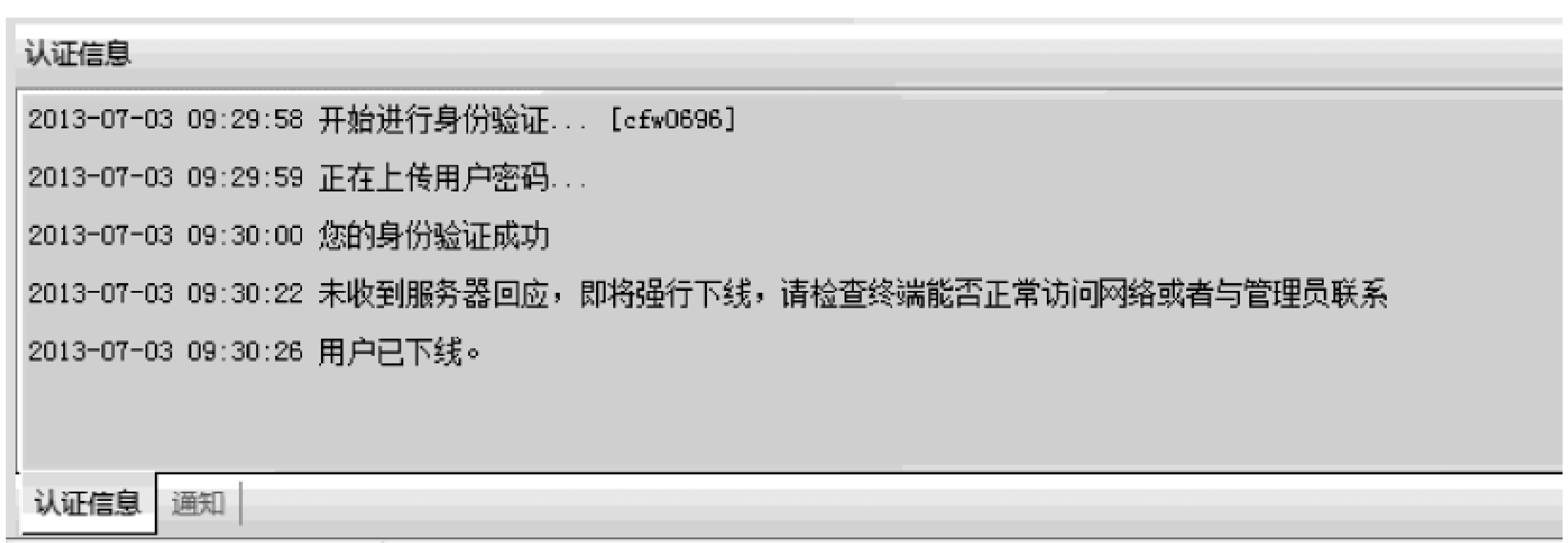


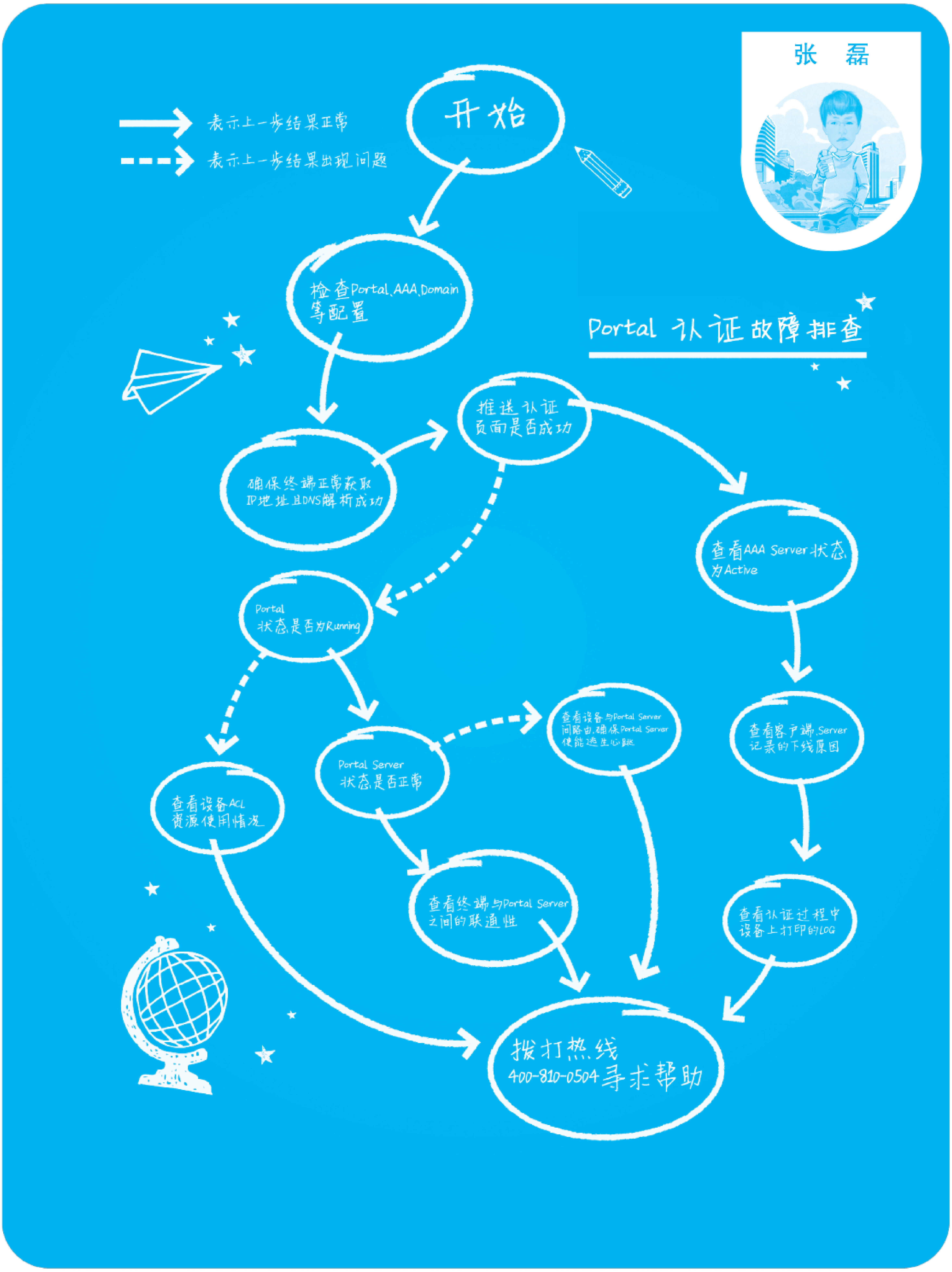
图 3-1　下线通知

(10) 查看认证过程中设备上的 Log 日志

用户认证失败时，设备上一般都会有相关的 Log 打印。

例如：向设备下发 ACL 时，设备上不存在该 ACL。

```
% Apr 26 13:44:47:017 2000 H3C 802.1x/5/DOT1X_SOP_ACL_FAILURE: -IfName =
GigabitEthernet1/0/2-UserName=123@h3c; The specified ACL does not exist.
```


张 磊
Portal 认证故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查Portal、AAA、Domain等配置
确保终端正常获取IP地址且DNS解析成功
推送认证页面是否成功
查看AAA Server状态为Active
Portal状态是否为Running
查看客户端、Server记录的下线原因
查看设备ACL资源使用情况
Portal Server状态是否正常
查看设备与Portal Server间路由，确保Portal Server使能逃生心跳
查看认证过程中设备上打印的LOG
查看终端与Portal Server之间的联通性
拨打热线400-810-0504寻求帮助

1. 开始

定位故障的思路是：以 Portal 认证流程为排查方向，先确保终端正常获取 IP 地址及 DNS 解析正常，然后查看终端 Web 页面是否可以重定向成功，再查看设备侧 Portal、Portal Server 相关状态是否正常，最后查看客户端、Server 上记录的下线原因及设备上的相关 Log。

2. 流程图相关操作说明

(1) 检查 Portal、AAA、Domain 等配置

检查 Portal、AAA、Domain 等配置，各部分注意事项如下。

① Portal 部分。在全局配置 Portal Server 且在三层接口下使能 Portal 认证。

例如：通过当前配置可确认在全局配置的 Portal Server 为 6.6.6.6 且在 VLAN 2 中使能了 Portal 认证。

```
#
portal server h3c ip 6.6.6.6 key cipher $c$3$t9t3GVbZEGTHeMLSVl41bB6l1fj4wQ== url http://6.6.6.6/portal
#
interface Vlan-interface2
 ip address 1.1.1.1 255.255.255.0
 portal server h3c method direct
#
```

② AAA 部分。配置 Radius Scheme 认证方案，指定认证、计费服务器。配置 Nas-Ip 且保证 Nas-Ip 到认证、计费服务器可达。同时保证 User-Name-Format 和 Server-Type 与 Radius Server 匹配。

例如：通过当前配置可知 Radius Scheme 的 Server-Type 为 Extended，User-Name-Format 为 Without-Domain。认证计费 Server 都为 1.1.1.1。

```
#
radius scheme h3c
 server-type extended
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 key authentication cipher $c$3$hmc/dsendG8XM8FKqsWbR7wjO0vF4A==
 key accounting cipher $c$3$PXWZGLZ4d64iZDVzdWn5nL2yJrv/uA==
 user-name-format without-domain
#
```

③ Domain 部分。在 Domain 视图下引用相应的 Radius Scheme 方案，认证授权方案必须同时指定。

例如：通过当前配置可知，Domain 下引用的 Radius Scheme 方案为 h3c。

```
#
domain h3c
```

```
authentication lan-access radius-scheme h3c
 authorization lan-access radius-scheme h3c
 accounting lan-access radius-scheme h3c
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
```

(2) 确保终端正常获取 IP 地址且 DNS 解析成功

Portal 根据终端发送的 HTTP 报文来进行重定向,必须确保终端在认证前通过 HHCP 或者静态配置的方式获取到正确的 IP 地址且 DNS 解析成功,这样浏览器才可以正常发送 HTTP 报文。

(3) 推送认证页面是否成功

在浏览器中访问任意网站,设备都会将其重定向至认证页面。

(4) Portal 状态是否为 Running

正常情况下 Portal 的运行状态为 Running。

命令:*display portal interface Vlan-interface vlan_id*

例如:通过命令查看,可以确认 Vlan 1 接口下的 Portal 功能是正常运行的。

```
<H3C>display portal   interface   Vlan-interface   1
 Interface portal configuration:
 Vlan-interface1:Portal running
 Portal server: imc
 Portal backup-group: None
 Authentication type: Direct
 Authentication domain:
 Authentication network:
 address : 0.0.0.0   mask : 0.0.0.0
```

(5) 查看设备 ACL 资源使用情况

查看设备是否有充足的 ACL 资源(IFP ACL)。如果设备 ACL 资源不足会导致在接口下使能 Portal 时提示 Portal 已经 Enable 但没有 Running。

命令:*display acl resource*

例如:通过命令查看,可以确认目前设备上 ACL 剩余:2816 条。

```
<H3C>display acl resource
 Interface:
    GE0/0/1 to GE0/0/28
---------------------------------------------------------------------------
  Type            Total       Reserved      Configured      Remaining
---------------------------------------------------------------------------
 VFP ACL          1024        0             0               1024
 IFP ACL          4096        1024          256             2816
 IFP Meter        2048        512           0               1536
 IFP Counter      2048        512           0               1536
 EFP ACL          512         0             0               512
 EFP Meter        256         0             0               256
 EFP Counter      512         0             0               512
```

(6) Portal Server 状态是否正常

正常情况下 Portal Server 的状态应该为 Up 或 N/A。

设备上 Portal Server 如果是处于 Down 状态,此时对 HTTP 报文不会进行重定向操作。

命令:*display portal server servername*

例如:通过命令查看,可以确认 Portal Server 处于正常的 Up 状态。

```
<H3C>display portal  server  imc
 Portal server:
  0)imc:
     IP              : 192.168.1.254
     VPN instance    : Not configured
     Port            : 50100
     Key             : h3c
     URL             : http://192.168.1.254/portal
     Status          : Up
```

(7) 查看设备与 Portal Server 间路由,确保 Portal Server 使能逃生心跳

设备上 Portal Server 如果是处于 Down 状态,说明 Portal 设备无法收到 Portal Server 的心跳报文,需要排查设备与 Portal Server 间路由且确保 Portal Server 使能逃生心跳且确保设备上配置的逃生心跳时间间隔应大于 IMC 上配置的时间间隔。

例如,从图 3-2 可知 Portal Server 上使能了逃生及用户心跳,时间分别为 20 秒。

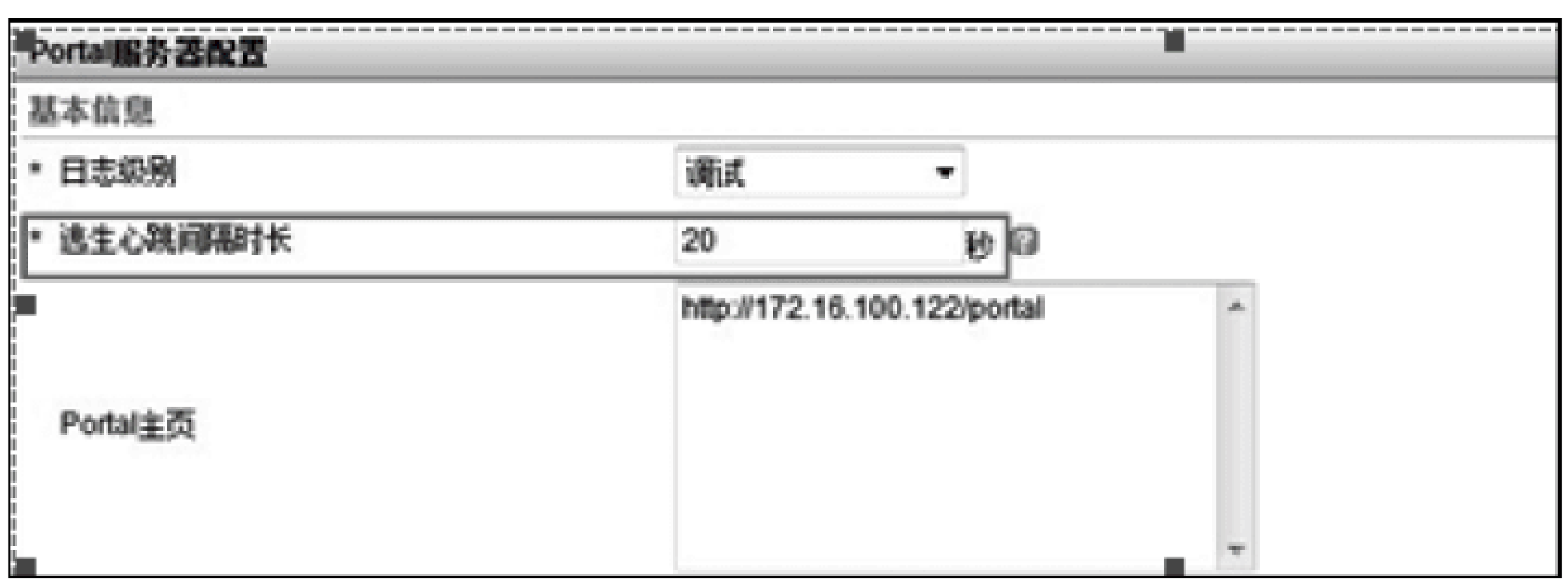


图 3-2　Portal Server 使能逃生心跳

(8) 确保终端与 Portal Server 之间的联通性

设备将页面重定向到 Portal Server 的页面后,后期终端与 Portal Server 之间交互的 HTTP 报文在设备是透明传输的。因此终端重定向成功的前提条件是必须保证终端与 Portal Server 之间的联通性。

(9) 查看 AAA Server 状态为 Active

确保 AAA Server 服务器的状态是 Active 的。

命令:*display radius scheme scheme-name*

例如:通过命令查看,可以确认 Scheme 方案中的主认证及计费服务器处于 Active 状态。

```
<H3C>display radius scheme imc
SchemeName   : imc
 Index : 0                          Type : standard
 Primary Auth Server:
    IP: 192.168.1.254               Port: 1812    State: active
    Encryption Key : imc
    VPN instance    : N/A
```

```
  Primary Acct Server:
    IP: 192.168.1.254              Port: 1813    State: active
    Encryption Key : imc
    VPN instance   : N/A
  ...
```

(10) 查看客户端、Server 上记录的下线原因

根据客户端及 Server 上常见的下线原因初步判断故障点。

例如，下线原因为 User Request，表示用户主动下线。如启用策略服务器的情况下，若 iNode 客户端与策略服务器通信的端口(Udp 9019)不通，iNode 会给出类似“未收到服务器回应，即将强行下线”的提示。

例如，图 3-3 是 iNode 客户端与策略服务器通信的端口不通导致的下线。



图 3-3 下线通知

(11) 查看认证过程中设备上打印的 Log

如果用户认证失败会有一些简单的原因提示。

① 下面的 Log 显示该用户的下线原因为 User Request，一般由客户端原因导致。

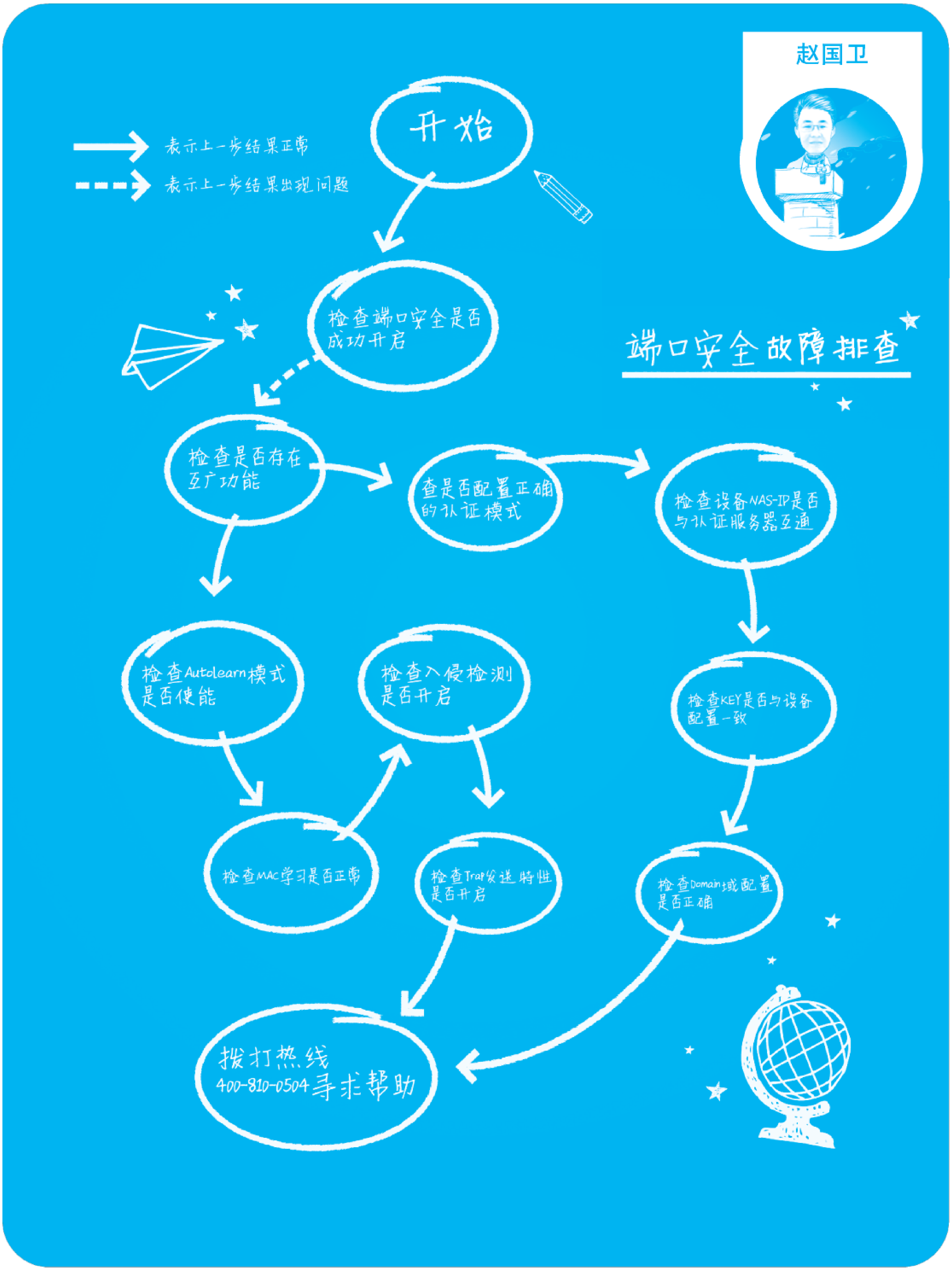
```
%Apr 11 19:13:11:074 2013 10504 PORTAL/5/PORTAL_USER_LOGOFF:
-UserName=[yuguanchenghome@sushe]-IPAddr=[10.11.1.56]-IfName=[Vlan-interface110]-
VlanID=[110]-MACAddr=[ec88-8f7b-ae87]-Reason=[User Request]; User logged off.
```

② 下面的 Log 显示该用户的下线原因为 Admin Reset，一般是由于人为操作强制用户下线的，或者设备上配置了在线用户同步功能，但是 IMC 上未使能该功能，导致设备收不到相关用户的在线信息，在一定的时间(默认 30 分钟左右)后设备强制该用户下线。

```
%Apr  9 20:45:50:263 2013 10504 PORTAL/5/PORTAL_USER_LOGOFF:
-UserName=[YTBTSk1ZZXojHEM1dAspc/AwEUA=YIMINGHOME@sushe]-IPAddr=[10.11.1.
156]-IfName=[Vlan-interface110]-VlanID=[110]-MACAddr=[f80f-4137-5ed1]-Reason=
[admin Reset]; User logged off.
```

③ 下面的 Log 表示，由于设备 ACL 资源不足导致用户上线不成功，需查看设备 ACL 资源使用情况。

```
%Nov 16 22:09:03:375 2011 ZG-7503-1 PORTAL/5/PORTAL_ACL_FAILURE: The number of
ACLs on the device has reached the maximum.
```


赵国卫
端口安全故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查端口安全是否成功开启
检查是否存在互斥功能
查是否配置正确的认证模式
检查设备NAS-IP是否与认证服务器互通
检查Autolearn模式是否使能
检查入侵检测是否开启
检查KEY是否与设备配置一致
检查MAC学习是否正常
检查Trap发送特性是否开启
检查Domain域配置是否正确
拨打热线
400-810-0504寻求帮助

1. 开始

端口安全模式可大致分为两大类：控制 MAC 学习类和认证类。所以定位故障思路是分别对这两大类可能产生的问题进行排查。

2. 流程图相关操作说明

(1) 检查端口安全是否成功开启

要使用端口安全功能，必须先在全局视图下使能端口安全功能。

在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。

命令：*port-security enable*

例如：在已经使能 dot1x 的情况下，通过命令使能端口安全功能会报错。

```
[H3C]port-security enable
 Error: Port-security can not be configured for dot1x is enabled.
```

(2) 检查是否存在互斥功能

端口安全和 dot1x 及 MAC 地址认证功能互斥，不能同时开启。

(3) 检查 Autolearn 模式是否使能

在配置 Autolearn 模式之前，需要先配置端口安全允许的最大 MAC 地址数。

命令：*port-security port-mode autolearn*

例如：在未配置端口安全允许学习的最大 MAC 地址数量情况下，端口下使能 Autolearn 模式会报错。

```
[H3C -GigabitEthernet1/0/20]port-security port-mode autolearn
 Error: Cannot enable autoLearn for max MAC address count is not set.
```

(4) 检查 MAC 地址学习是否正常

开启端口安全 Autolearn 模式之后，端口会自动学习 MAC 直到达到端口安全允许的最大 MAC 数量，如果 MAC 地址不能正常学习，先检查是否已经达到最大数量。

命令：*displayport-security interface GigabitEthernet interface-number*

例如：通过此命令可以查看到在使能端口安全 Autolearn 模式，端口 G1/0/20 配置的最大自动学习 MAC 数量为 20。

```
[lsw-center]display port-security interface GigabitEthernet 1/0/20
 Equipment port-security is enabled
 Trap is disabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:
 GigabitEthernet1/0/20 is link-down
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is NoAction
```

```
Max MAC address number is 20
Stored MAC address number is 0
Authorization is permitted
Security MAC address learning mode is sticky
Security MAC address aging type is absolute
```

（5）检查入侵检测是否开启

如果发现开启端口安全的端口不能通信，可以检查设备是否开启了入侵检测特性。

设备上入侵检测默认是关闭的。

开启入侵检测后，会触发下面三种安全措施。

① blockmac：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中，源 MAC 地址为阻塞 MAC 地址的报文将被丢弃。此 MAC 地址在被阻塞 3 分钟（系统默认，不可配）后恢复正常。

② disableport：表示将收到非法报文的端口永久关闭。

③ disableport-temporarily：表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 *port-security timer disableport* 命令配置。

命令：*display port-security interface GigabitEthernet interface-number*

例如：通过此命令可以查看到端口 G1/0/20 采用了 disableport 的入侵检测模式。

```
[lsw-center]display port-security interface GigabitEthernet 1/0/20
 Equipment port-security is enabled
 Trap is disabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:
 GigabitEthernet1/0/20 is link-down
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePort
   Max MAC address number is 20
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

（6）检查 Trap 发送特性是否开启

如果端口上发生关键事件时没有触发对应的 Trap 信息，需要检查 Trap 发送特性是否开启。

设备上默认 Trap 发送特性是关闭的。Trap 发送包括下面几种情况。

① addresslearned：端口学习到新 MAC 地址时发出告警信息。

② dot1xlogfailure/dot1xlogon/dot1xlogoff：802.1x 用户认证失败/认证成功/下线时发出告警日志。

③ ralmlogfailure/ralmlogon/ralmlogoff：MAC 地址认证用户认证失败/认证成功/下线时发出告警信息。

④ intrusion：发现非法报文时发出告警信息。

命令：*displayport-security interface interface-number*

例如：通过命令可以查看到对应的 addresslearned 的 Trap 发送特性已经开启。

```
[H3C] display port-security interface g1/0/20
 Equipment port-security is enabled
 AddressLearned trap is enabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:
 GigabitEthernet1/0/20 is link-down
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePort
   Max MAC address number is 20
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

（7）检查是否配置正确的认证模式

端口安全认证类功能提供了更为灵活的认证模式。可灵活选择不同的 dot1x 和 MAC 认证方式。要根据客户的实际应用情况，选择适当的认证模式。如果认证未符合预期结果，则需先排查认证模式是否正确。

命令：*display port-security interface*

例如：查看到端口 G1/0/21 当前认证模式为 user Login。

```
[H3C]display port-security int GigabitEthernet 1/0/21
 Equipment port-security is enabled
 AddressLearned trap is enabled
 AutoLearn aging time is 0 minutes
 Disableport Timeout: 20s
 OUI value:

 GigabitEthernet1/0/21 is link-down
   Port mode is userLogin
   NeedToKnow mode is disabled
   Intrusion Protection mode is NoAction
   Max MAC address number is not configured
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

（8）检查设备 NAS-IP 是否与认证服务器互通

确保设备与认证服务器之间 IP 和端口可达。

（9）检查 KEY 是否与设备配置一致

检查设备 KEY 配置是否与认证服务器配置的一致。

（10）检查 Domain 域配置是否正确

H3C 设备默认的 Domain 域是 system，如果不指定域后缀，用户认证的时候都会到默认的 system 域去认证，要检查默认域是否配置为用户的认证域。另外不管是否存在计费和授权，在 Domain 下都要同时指定认证、授权、计费的 Radius-scheme，三者同配，缺一不可。

命令：*domain default enable h3c*

例如：查看配置中认证、授权、计费的引用，并配置用户认证域 H3C 为默认的 Domain。

```
[H3C]domain h3c
[H3C-isp-h3c]display this
#
domain h3c
 authentication default radius-scheme imc
 authorization default radius-scheme imc
 accounting default radius-scheme imc
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable

[H3C]domain default enable h3c
```


赵国卫
开始
查看用户是否在线
MAC地址认证故障排查
检查MAC地址认证用户名格式
检查NAS-IP配置是否正确
检查设备NAS-IP与Radius Server是否互通
检查Radius进程是否正常启动
检查是否下发了设备不支持的属性
检查key与Radius server是否一致
检查Domain或Radius Scheme配置是否正确
查看认证失败或下线原因
查看Radius Scheme状态信息
查看MAC认证静默时间配置是否合理
拨打热线 400-810-0504寻求帮助
表示上一步结果正常
表示上一步结果出现问题

03 交换技术 › 3.2 安全接入 › 3.2.4 MAC 地址认证故障排查 › 步骤详解

1. 开始

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，是基于 C/S 架构的，客户端和服务器都要排查，所以定位故障的思路是分别检查用户接入设备和远端负责对用户进行认证的 Radius 服务器。

2. 流程图相关操作说明

(1) 查看用户是否在线

在设备上查看用户是否在线。

命令：*display connection*

display connection ucibindex uncibindex-number

例如：通过命令查看在线用户信息，可以确认用户名 admin 的用户已经在线，其用户索引为 134，后面跟 ucibindex 参数及对应用户的索引 134 可查看对应在线用户 0026-B9AA-C9FB 的详细信息。

```
<H3C>display connection
Slot:  1
Index=134 , Username=0026-B9AA-C9FB@system
IP=10.153.47.44
IPv6=N/A
<H3C>display connection ucibindex 134
Slot:  1
Index=134, Username=0026-B9AA-C9FB@system
IP=10.153.47.44
IPv6=N/A
Access=0026-B9AA-C9FB, AuthMethod=PAP
Port Type=Virtual , Port Name=N/A
Initial VLAN=N/A, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2013-05-06 14:08:43 ,Current=2013-05-06 14:50:47 ,Online=00h42m04s
Total 1 connection matched.
```

(2) 检查 MAC 地址认证用户名格式

检查 MAC 地址认证用户名格式是否合理，默认情况下，使用用户的源 MAC 地址做用户名与密码，其中字母为小写，MAC 地址不带连字符"-"，可以采用命令 *mac-authentication user-name-format* 来配置用户名格式。

(3) 检查设备 NAS-IP 与 Radius Server 是否互通

确保设备到 Radius ServerIP 地址和端口可达。

(4) 检查 Key 与 Radius Server 是否一致

查看设备侧配置的 Radius Key 和 Radius Server 侧配置的 Key 是否一致。

命令：*display this*

例如：通过命令查看 Key 配置。

```
[H3C]radius scheme imc
[H3C-radius-imc]display this
 radius scheme imc
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 key authentication h3c
 key accounting h3c
 user-name-format without-domain
```

（5）检查 Domain 或 Radius Scheme 配置是否正确

如果设备要下发 H3C 私有 Radius 属性，则需要将服务类型配置为 extended。

命令：*display this*

例如：Radius Scheme 视图下查看服务类型是否为 extended。

```
[H3C-radius-imc]display this
 server-type extended
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 secondary authentication 1.1.1.17
 secondary accounting 1.1.1.17
```

我们设备默认的 domain 域是 system，如果不指定域后缀，用户认证的时候都会到默认的 system 域去认证，要检查默认域是否配置为用户的认证域。另外不管是否存在计费和授权，在 domain 下都要同时指定认证、授权、计费的 Radius-scheme，三者同配，缺一不可。

命令：*display this*

domain default enable h3c

例如：查看配置中认证、授权、计费的引用，并配置用户认证域 H3C 为默认的 domain。

```
[H3C]domain h3c
[H3C-isp-h3c]display this
#
 domain h3c
 authentication default radius-scheme imc
 authorization default radius-scheme imc
 accounting default radius-scheme imc
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable

[H3C]domain default enable h3c
```

（6）查看 Radius Scheme 状态信息

不仅要确认到 Radius 服务器路由可达，还要确认对应认证、计费、授权服务器是否端口可达。

命令：*display raidus scheme imc*

例如：通过命令查看 radius scheme 状态信息，确认其状态为 active。

```
<H3C>display radius scheme imc
SchemeName   : imc
  Index : 1                          Type : extended
  Primary Auth Server:
    IP: 1.1.1.1                            Port: 1812    State: active
    Encryption Key : N/A
    VPN instance   : N/A
    Probe username : N/A
    Probe interval : N/A
  Primary Acct Server:
    IP: 1.1.1.1                            Port: 1813    State: active
    Encryption Key : N/A
    VPN instance   : N/A
```

（7）查看 MAC 认证静默时间配置是否合理

若 MAC 地址认证失败，此 MAC 会被加为静默 MAC，来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

命令：*mac-authentication timer quiet*

（8）NAS-IP 配置是否正确

检查服务器侧是否配置了 NAS-IP 以及配置的 NAS-IP 是否与设备指定的 NAS-IP 一致。如图 3-4 所示，这里设备的 NAS-IP 为 10.1.1.200，则在 iMC 侧配置的接入设备 IP 也要是 10.1.1.200。



图 3-4　查看设备接入配置信息

（9）Radius 进程是否正常启动

查看服务器侧 Radius 进程是否正常启动，是否存在应用端口号被占用的情况，以及是否配置 Radius 代理。

（10）是否下发了设备不支持的属性

服务器可以下发各种 Radius 属性，有些属性对格式有要求，要注意下发的属性格式在设

备上是否能够支持。如果下发了设备不支持的属性会导致认证失败。常用的 Radius 属性有：用户权限、ACL、VLAN、CAR 限速。常见的 Radius 属性如表 3-1 所示。

表 3-1 常见的 Radius 属性

属 性 名	属性编号	格式(Text，String，Address，Integert)	具 体 定 义
Input-Peak-Rate	1	Integer	用户接入到 NAS 的峰值速率，以 bps 为单位
Input-Average-Rate	2	Integer	用户接入到 NAS 的平均速率，以 bps 为单位
Input-Basic-Rate	3	Integer	用户接入到 NAS 的基本速率，以 bps 为单位。(这个域目前没有意义，建议不要使用)
Output-Peak-Rate	4	Integer	从 NAS 到用户的峰值速率，以 bps 为单位
Output-Average-Rate	5	Integer	从 NAS 到用户的平均速率，以 bps 为单位
Output-Basic-Rate	6	Integer	从 NAS 到用户的基本速率，以 bps 为单位。(这个域目前没有意义，建议不要使用)
Exec-Privilege	29	Integer	EXEC 用户优先级。 对于 EXEC 用户，用户的优先级。用来设置 EXEC 用户的优先级。RADIUS 服务器在认证接收报文中，可以用属性 Exec_Privilege 携带 EXEC 用户的优先级。该属性是针对管理用户的设置
Tunnel-Private-Group-ID	81	Integer	参照 RFC 定义，用作 VPDN 组号 说明：为了与以前设备实现的方式兼容，该属性取值为[1-4094]下发给设备的值的类型为 Integer，其他值的类型为 String
Tunnel-Assignment-ID	82	Integer	参照 RFC 定义
Filter-ID	11	String (协议中规定此属性类型为 Text)	访问控制列表的名字。不同产品实现定义不同。建议客户端不要对 Radius 服务器上定义的 Filter-Id 的名字做限制，具体的规则在客户端上进行配置 MA5200：ACLGroup@InterGroup，其中 ACLGroup 可以是 ACL 组号，也可以为是 ACL 组名；InterGroup 及既可以是 InterGroup 组号，也可以是 InterGroup 组名。如果带有多个 Filter-ID，则只有最后一个 Filter-ID 起作用，因此建议只带一个 Filter-ID

(11) 查看认证失败或下线原因

Radius 服务器都会有对应的日志记录用户认证失败或下线的原因。常见的下线原因，可以参考下面的说明。

```
Acct-Terminate-Cause      User-Request          1
```

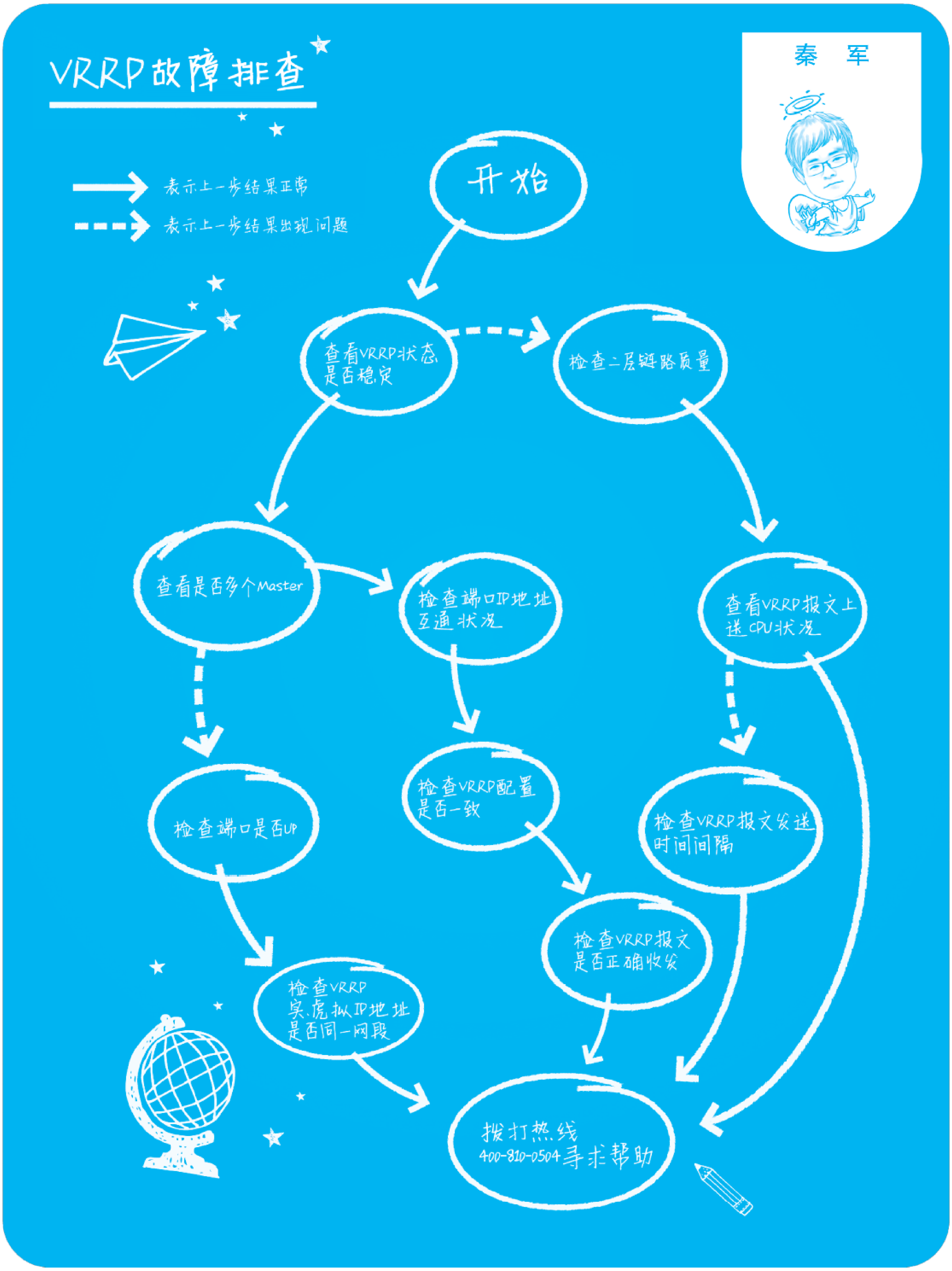
#这种情况，属于用户请求下线，一般为客户端主动下线，需要检查客户端。

```
Acct-Terminate-Cause      Idle-Timeout          4
```

#这种情况为闲置超时下线。

```
Acct-Terminate-Cause      Session-Timeout       5
```

#这种情况为会话超时，一般为计费不足或者进行了时间段限制。


VRRP故障排查
秦 军
表示上一步结果正常
表示上一步结果出现问题
开始
查看VRRP状态是否稳定
检查二层链路质量
查看是否多个Master
检查端口IP地址互通状况
查看VRRP报文上送CPU状况
检查端口是否UP
检查VRRP配置是否一致
检查VRRP报文发送时间间隔
检查VRRP报文是否正确收发
检查VRRP实虚拟IP地址是否同一网段
拨打热线 400-810-0504寻求帮助

1. 开始

定位故障的思路是：首先观察备份组 VRRP 状态是否稳定。如果状态稳定，则检查 VRRP 接口实 IP 地址能否互通，再检查 VRRP 配置是否正确，最后查看协议报文的发送状况；如果状态频繁切换，则检查收发 VRRP 报文所在 VLAN 的二层链路是否稳定，再检查 CPU 占用率是否正常，最后检查 VRRP 报文发送时间间隔是否过短。

2. 流程图相关操作说明

(1) 查看 VRRP 状态是否稳定

路由器在备份组中的状态可以为 Master、Backup 和 Initialize。检查 VRRP 状态是否存在 Master/Backup 频繁切换的情况。

命令：*display vrrp*

例如：通过命令多次查看，可以确认路由器的 VRRP 状态。

```
<H3C>display vrrp
 IPv4 Standby Information:
     Run Mode        : Standard
     Run Method      : Virtual MAC
 Total number of virtual routers : 1
 Interface    VRID   State      Run     Adver   Auth     Virtual
                                Pri     Timer   Type     IP
 -----------------------------------------------------------------
 Vlan1        1      Backup     100     1       Simple   1.1.1.254
```

(2) 查看是否多个 Master

分别查看每台路由器备份组的 VRRP 状态信息，是否备份组中存在多个路由器 VRRP 状态处于 Master。

(3) 检查端口是否 Up

检查运行 VRRP 的 VLAN 虚接口是否 Up。

命令：*display interface interface-type interface-number*

例如：通过命令查看 VLAN 1 三层虚接口状态是否 Up。

```
<H3C>display interface Vlan-interface 1
Vlan-interface1 current state:Down
Line protocol current state:Down
Description: Vlan-interface1 Interface
...
```

(4) 检查 VRRP 实、虚拟 IP 地址是否同一网段

确保运行 VRRP 的端口 Up 的前提下，查看 VRRP 的虚拟 IP 是否与端口实 IP 在同一网段。

例如：查看运行 VRRP 的端口下实 IP 地址与虚拟 IP 地址。

```
[H3C]display current-configuration interface Vlan-interface 1
#
interface Vlan-interface1
 ip address 1.1.1.252 255.255.255.0
 vrrp vrid 1 virtual-ip1.1.100.254
 vrrp vrid 1 virtual-ip 1.1.100.254
```

(5) 检查端口 IP 地址互通状况

如果带接口源地址互 ping VRRP 接口的实 IP 地址不通，主要检查以下内容。

① 检查接口是否 Up，链路是否故障。

② 如果物理接口是 access 端口，是否与 VRRP 备份组属于同一 VLAN；如果是 trunk 或者 hybrid 端口，端口的 PVID 是否一致，是否允许 VRRP 备份组所在 VLAN 通过。

③ 端口下是否开启了认证、ACL 过滤等安全功能。

(6) 检查 VRRP 配置是否一致

主要检查内容包括：运行模式、VRID、Virtual IP、VRRP 报文发送间隔时间、抢占模式、认证方式和认证字的配置是否相同。

命令：*display vrrp verbose interface interface-type interface-number*

例如：通过命令查看，观察 Master 和 Slave 的相关参数是否一致。

```
<H3C>display vrrp verbose interface Vlan-interface 1
 IPv4 Standby Information:
     Run Mode          :Standard
     Run Method        : Virtual MAC
 Total number of virtual routers on interface Vlan1 : 1
   Interface Vlan-interface1
     VRID              :1               Adver Timer  : 2
     Admin Status      : Up             State        : Master
     Config Pri        : 120            Running Pri  : 120
     Preempt Mode      :Yes             Delay Time   : 0
     Auth Type         :Simple          Key          : ******
     Virtual IP        :1.1.1.254
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 1.1.1.253
```

(7) 检查 VRRP 报文是否正确收发

在中间设备或互连接口做流量统计，检查是否有 VRRP 报文从接口发出或接收。如果要检查是否正常发出了 VRRP 报文，则在物理接口的 Outbound 方向进行流量统计；如果要检查是否正常接收了 VRRP 报文，则在接口的 Inbound 方向进行流量统计。

命令：*display qos policy interface interface-type interface-number*

例如：通过匹配源地址为 1.1.1.252、目的地址为 224.0.0.18、协议号为 112 的 VRRP 报文，对这一类型的报文在接口下做 Inbound 方向流量统计，观察 VRRP 报文的接收情况是否正常。

```
[H3C]display current-configuration
...
acl number 3000
 rule0 permit 112 source 1.1.1.252 0 destination 224.0.0.18 0
#
```

```
[H3C]display qos policyinterface GigabitEthernet 3/0/1
  Interface: GigabitEthernet3/0/1
  Direction:Inbound
  Policy:ACT
   Classifier:ACT
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior:ACT
       Accounting Enable:
         51 (Packets)
```

(8) 检查二层链路质量

① 使用 VRRP 接口的实 IP 地址互 ping 时是否有回应超时。

② 检查互连物理端口是否有错误报文的增长。

③ 检查链路状况是否有震荡,是否有端口频繁 Up/Down。

④ 如果是光介质,检查光衰减是否在正常范围之内。

(9) 查看 VRRP 报文上送 CPU 状况

为了防止协议报文对 CPU 的攻击,设备根据上 CPU 的不同类型的报文设置了限速值,如果网络中存在大量 VRRP 组或存在恶意攻击,使得每秒上送 CPU 的 VRRP 报文超过阈值,那么就丢弃超出阈值的 VRRP 报文,从而可能造成某些 VRRP 组震荡。通过多次查看 CPU 利用率,可以判断当前的 CPU 状态是否正常。如果 CPU 占用率超过 90%,则说明对 CPU 占用率过高,需要先对 CPU 任务处理进行排查;否则,打开 VRRP 报文的调试开关,观察 VRRP 报文的交互过程。

命令:*display cpu-usage*

例如:查看当前的 CPU 利用率。

```
[H3C]display cpu-usage
Slot 1 CPU usage:
      94% in last 5 seconds
      90% in last 1 minute
      88% in last 5 minutes
```

命令:*debugging vrrp packet*

例如:通过调试信息判断,VRRP 报文接收间隔与通告时间一致,没有出现丢包。

```
<H3C>terminal debugging
<H3C>terminal monitor
<H3C>debugging vrrp packet
 *Jul 30 07:39:21:704 2013 H3C VRRP/7/DebugPacket:
 Received Advertisement message from 1.1.1.252 on Vlan-interface1.
 VRID: 1   Pri: 110   Adver timer:1 secs

 *Jul 30 07:39:22:754 2013 H3C VRRP/7/DebugPacket:
 Received Advertisement message from 1.1.1.252 on Vlan-interface1.
 VRID: 1   Pri: 110   Adver timer:1 secs

 *Jul 30 07:39:23:809 2013 H3C VRRP/7/DebugPacket:
 Received Advertisement message from 1.1.1.252 on Vlan-interface1.
 VRID: 1   Pri: 110   Adver timer:1 secs
```

（10）检查 VRRP 报文发送时间间隔

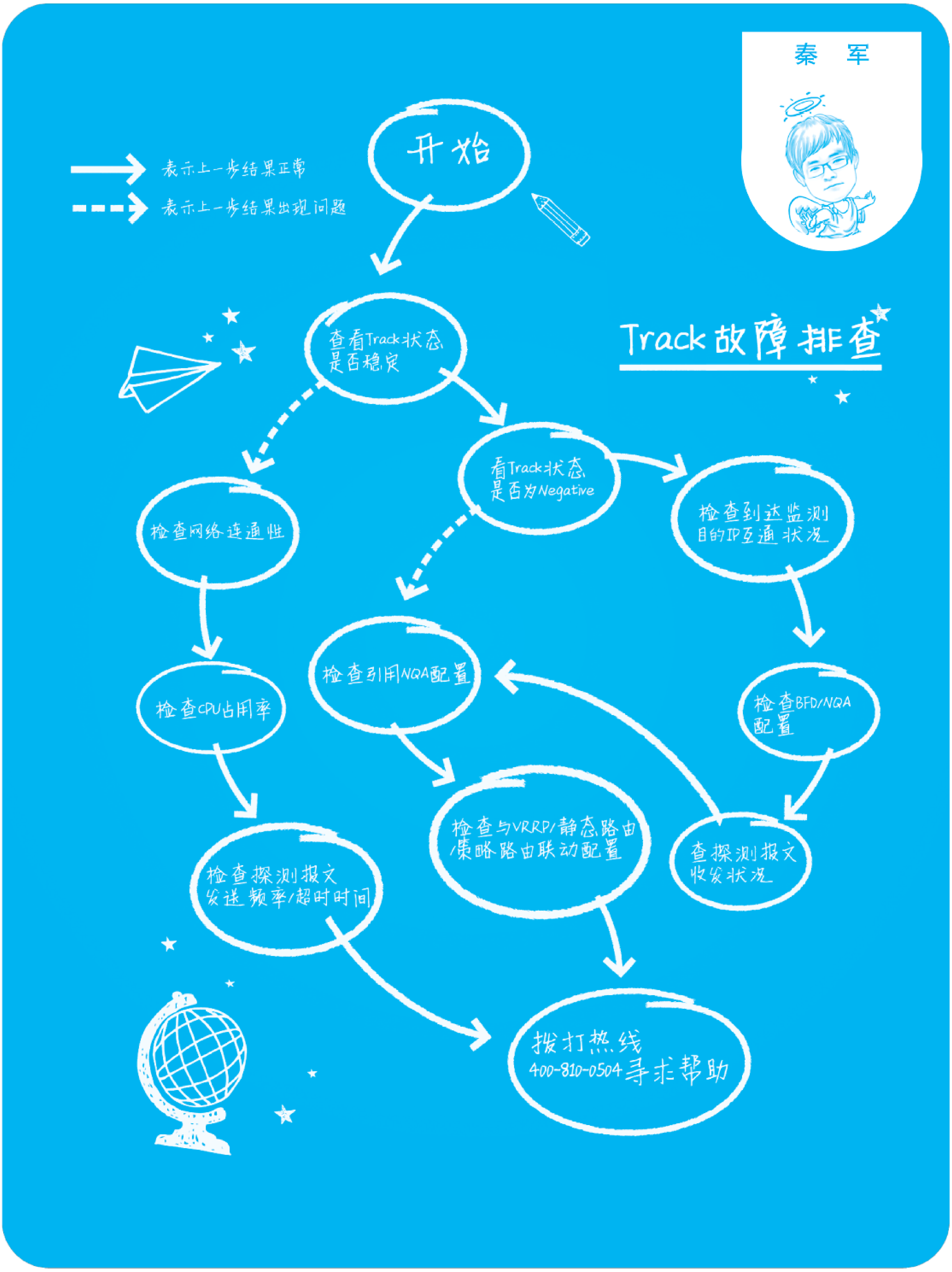
根据网络的流量大小、设备的性能、链路质量状况等因素，合理配置 VRRP 通告报文的发送间隔，如果时间间隔过短，可能造成主备状态的频繁切换。如果配置的 VRRP 组数较多时，建议将各组 VRRP 通告报文发送间隔参数按照质数的方式分开设置，以避免同一时刻发出大量 VRRP 报文导致对端来不及处理以致 VRRP 状态错误。比如第一组配置为 2 秒，第二组配置为 3 秒，第三组配置为 5 秒，依此类推。

说明：VRRP 通告报文发送时间间隔增加后，设备的抢占等待时间也会增加。

命令：vrrp vrid *virtual-router-id* timer advertise *adver-interval*

例如：在运行 VRRP 的接口下修改 VRRP 通告报文的发送间隔为 3 秒。

```
<H3C>display vrrp interface Vlan-interface 1 vrid 1
 IPv4 Standby Information:
     Run Mode      : Standard
     Run Method    : Virtual MAC
 Interface         VRID    State     Run     Adver   Auth     Virtual
                                     Pri     Timer   Type     IP
 ---------------------------------------------------------------------
 Vlan1             1       Master    120     3       Simple   1.1.1.254
```


秦 军
Track故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看Track状态是否稳定
看Track状态是否为Negative
检查到达监测目的IP互通状况
检查BFD/NQA配置
查探测报文收发状况
检查网络连通性
检查CPU占用率
检查探测报文发送频率/超时时间
检查引用NQA配置
检查与VRRP/静态路由/策略路由联动配置
拨打热线 400-810-0504寻求帮助

1. 开始

定位故障的思路是：首先观察 Track 项状态是否稳定。如果 Track 项状态频繁切换，则检查网络质量、CPU 占用率以及探测报文发送频率/超时时间的设置；如果 Track 项稳定在 Negative 状态，则检查互联网络状态、BFD/NQA 的配置以及探测报文的收发状况；如果 Track 项稳定在其他状态，则检查联动的配置。

2. 流程图相关操作说明

(1) 查看 Track 状态是否稳定

Track 项的状态分为 Positive、Negative 和 Invalid。查看 Track 项的状态是否存在 Positive/Negative 频繁切换的情况。

命令：*display track track-entry-number*

例如：通过命令查看 Track 1 的当前状态。

```
[H3C]display track 1
Track ID: 1
  Status:Positive
  Duration: 0 days 0 hours1 minutes 22 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    BFD session:
    Packet type: Echo
    Interface   : Vlan-interface1
    Remote IP   : 1.1.1.253
    Local IP    : 1.1.1.252
```

(2) 检查网络连通性

① 使用探测报文的源、目的地址互 ping 时是否有回应超时。

② 检查互连端口是否有错误报文的增长。

③ 检查链路状况是否有震荡，是否有端口频繁 Up/Down。

④ 如果是光介质，检查光衰减是否在正常范围之内。

(3) 检查 CPU 占用率

一般情况下，CPU 利用率超过 90%时可能会导致探测报文上送 CPU 丢包，这时需要排查 CPU 占用率高的原因。

命令：*display cpu-usage*

例如：查看设备的 CPU 占用率。

```
<H3C>display cpu-usage
Slot1 CPU usage:
      92% in last 5 seconds
      90% in last 1 minute
      81% in last 5 minutes
```

(4) 检查探测报文发送频率/超时时间

根据网络的流量大小、设备的性能、链路质量状况等因素,合理配置探测报文的发送间隔以及失效时间。

① 修改 BFD 探测报文的发送间隔和允许失效的最大个数。

命令: *bfd min-echo-receive-interval value*

bfd detect-multiplier value

例如:配置 bfd echo 报文发送间隔为 1000ms,最多允许 6 个报文失效。

```
<H3C>display bfd session verbose
 Total session number: 1     Up session number: 1     Init mode: Active
 IPv4 session working under Echo mode:
       Local Discr: 35
          Source IP: 1.1.1.252            Destination IP: 1.1.1.253
    Session State: Up                           Interface: Vlan-interface1
   Min Recv Inter:1000ms              Act Trans Inter: 1000ms
Act Detect Inter:6000ms              Running Up for: 00:10:47
      Connect Type: Direct                    Board Num: 2
            Protocol: Track
          Diag Info: No Diagnostic
```

② 修改 NQA 探测报文的发送间隔和允许连续的探测失败次数。

命令: frequency *interval*

reaction *item-number* checked-element probe-fail threshold-type consecutive *consecutive-occurrences* action-type trigger-only

例如:配置 NQA 探测报文发送间隔为 1500ms,最多允许连续 5 个报文失效。

```
[H3C-nqa-admin-test-icmp-echo]display this
#
  type icmp-echo
  frequency 1500
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
```

(5) 查看 Track 状态是否为 Negative

通过命令查看 Track 项状态,确定稳定在 Negative 状态,还是稳定在 Positive 或者 Invalid 状态。

命令: *display track track-entry-number*

例如:通过命令查看 Track 1 的当前状态。

```
[H3C]display track 1
Track ID: 1
  Status:Negative
  Duration: 0 days 0 hours 0 minutes 2 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

(6) 检查到达监测目的 IP 互通状况

如果互 ping 监测的目的 IP 地址不通,主要检查以下内容。

① 检查接口是否 Up，链路是否故障。

② 检查二层接口是否允许探测报文通过。

③ 端口下是否开启了认证、ACL 过滤等安全功能。

(7) 检查 BFD/NQA 配置

① 配置 Track 与 BFD 联动时，VRRP 备份组的虚拟 IP 地址不能作为 BFD 会话探测的 Local IP 和 Remote IP。

② 对于 BFD Echo 模式，必须 BFD Echo 报文的源 IP 地址，这一 IP 地址不属于该设备任何一个接口所在网段。

③ 对于 NQA，检查是否配置了测试组进行测试的启动时间和持续时间，并检查系统时间是否在<启动时间>到<启动时间＋持续时间>范围之内。

④ 当 Track 与 BFD 联动时，检查 BFD 会话状态是否正常。

命令：*display bfd session verbose*

例如：通过命令查看 BFD 会话的当前状态。

```
<H3C>display bfd session verbose
 Total Session Num: 1                Init Mode: Active
 IPv4 Session Working Under Echo Mode:
 Local Discr: 36
 Source IP: 1.1.1.252                Destination IP: 1.1.1.253
 Session State:Up                    Interfa ce: Vlan-interface1
 Min Recv Inter: 400ms               Act Trans Inter: 400ms
 Act Detect Inter: 2000ms            Running Up for: 00:00:09
 Connect Type: Direct                Board Num: 1
 Protocol: Track
 Diag Info: No Diagnostic
```

⑤ 当 Track 与 NQA 联动时，检查 NQA 测试组的监测结果。

命令：*display nqa result admin-name operation-tag*

例如：通过命令多次查看，如果红色部分数字全为 0，则说明 NQA 检测失败。

```
[H3C]display nqa result admin test
  NQA entry (admin admin, tag test) test results:
    Destination IP address:1.1.1.253
      Send operation times:1                Receive response times: 1
      Min/Max/Average round trip time:9/9/9
      Square-Sum of round trip time:81
      Last succeeded probe time:2012-11-08 17:20:11.8
…
```

(8) 检查探测报文收发状况

① 对于 BFD 探测报文，匹配源地址为 BFD Echo-Source-IP，源、目的端口为 3785 的 UDP 报文；对于 NQA 探测报文，根据配置的源、目的 IP 地址及报文类型匹配报文。

命令：*display qos policy interface interface-type interface-number*

例如：通过匹配指定的源、目的 IP、协议类型为 ICMP 的 NQA 探测报文，对这一类型的报文在接口下做流量统计，观察报文的收发情况是否正常。

```
[H3C]display current-configuration
…
```

```
acl number 3000
rule 0 permit icmp source 1.1.1.252 0 destination 1.1.1.253 0
#
[H3C]display qos policy interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  Direction:Inbound
  Policy: acc
   Classifier: acc
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: acc
       Accounting Enable:
         26152 (Packets)
```

说明：在封装探测报文设备的出接口做流量统计，统计不到探测报文数据为正常现象。

② 命令：*display nqa statistics*

例如：通过命令查看 NQA 报文统计信息，检查是否收到或发出了探测报文。

```
[H3C]display nqa statistics
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 1.1.1.253
      Start time: 2012-11-08 13:05:02.2
      Life time: 1351 seconds
      Send operation times:7045            Receive response times: 6620
      Min/Max/Average round trip time: 1/51/5
      Square-Sum of round trip time: 274288
    Extended results:
      Packet loss in test: 6%
      Failures due to timeout:425
      Failures due to disconnect: 0
    Reaction statistics:
      Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
      2       probe-fail        consecutive      7044          425
```

(9) 检查引用 NQA 配置

配置 Track 项时，如果引用了错误的 NQA 测试组，则该 Track 项的状态为 Invalid。

例如：Track 项错误的引用了 NQA 测试组 admin test Reaction 1 导致 Track 项状态为 Invalid。

```
[H3C]display track 1
Track ID: 1
  Status:Invalid
  Duration: 0 days 0 hours 1 minutes 9 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry:admin test
    Reaction:1
[H3C]display nqa reaction counters admin test
  NQA entry (admin admin, tag test) reaction counters:
    Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
    2       probe-fail        consecutive      833           73
```

（10）检查与 VRRP/静态路由/策略路由联动配置

如果 Track 项状态发生变化时，无法与应用模块联动，检查需要关联的 Track 项是否已创建或与应用模块关联的 Track 项是否正确。

例如：查看配置的静态路由是否与 Track 项正确关联。

```
[H3C]display current-configuration | include ip route
 ip route-static 100.1.1.0 255.255.255.0 10.1.1.253 track 1

[H3C]display track all
Track ID:1
  Status: Positive
  Duration: 0 days 0 hours 0 minutes 13 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 2
```


RRPP故障排查
王 京
Hey There
开始
查看RRPP协议和RRPP环是否使能
查看RRPP的域ID配置是否相同
查看控制VLAN和保护VLAN配置是否相同
查看环上各个节点的端口状态
查看环上各个节点的协议报文收发情况
拨打热线 400-810-0504寻求帮助
表示上一步结果正常
表示上一步结果出现问题

1. RRPP 问题排查

定位故障的思路是：查看 RRPP 协议和 RRPP 环是否使能，查看 RRPP 的域 ID 配置是否相同，查看控制 VLAN 和保护 VLAN 配置是否相同，查看环上各个节点的端口状态是否正常，查看环上各个节点的协议报文收发情况。

2. 流程图相关操作说明

(1) 查看 RRPP 协议和 RRPP 环是否使能

查看环上各个节点 RRPP 协议和 RRPP 环是否使能，只有当 RRPP 协议和 RRPP 环都使能之后，当前设备的 RRPP 域才能被激活。

命令：*display rrpp brief*

例如：通过命令查看，可以确认 RRPP 协议已经使能，RRPP 环 1 已经使能。

```
<H3C>display rrpp brief
Flags for Node Mode :
M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge

RRPP Protocol Status: Enable
Number of RRPP Domains:1

Ring   Ring    Node   Primary/Common   Secondary/Edge   Enable
ID     Level   Mode   Port             Port             Status
-------------------------------------------------------------------
1      1       M      GE1/0/1          GE1/0/2          Yes
```

(2) 查看 RRPP 的域 ID 配置是否相同

查看环上各个节点 RRPP 的域 ID 配置是否相同，域 ID 用来唯一标识一个 RRPP 域，在同一 RRPP 域内的所有节点上应配置相同的域 ID。

命令：*display current-configuration | include rrpp domain*

例如：通过命令查看，可以确认 RRPP 的域 ID 为 1。

```
<H3C>display current-configuration | include rrpp domain
rrpp domain  1
```

(3) 查看控制 VLAN 和保护 VLAN 配置是否相同

查看环上各个节点的控制 VLAN 和保护 VLAN 配置是否相同，在同一 RRPP 域内的所有节点上应配置相同的控制 VLAN 和相同的保护 VLAN。

命令：*display stp region-configuration*

例如：通过命令查看，可以确认 RRPP 的控制 VLAN 为 4000，保护 VLAN 的 MSTI 为 0，且 MSTI 0 所映射的 VLAN 列表是 1 to 4094。

```
[H3C-rrpp-domain1]dis this
#
rrpp domain 1
 control-vlan  4000
```

```
protected-vlan reference-instance  0
#

<H3C>dis stp region-configuration
 Oper configuration
   Format selector        :0
   Region name            :c4cad9c05138
   Revision level         :0
   Configuration digest   :0xac36177f50283cd4b83821d8ab26de62

   Instance   Vlans Mapped
      0        1 to 4094
```

（4）查看环上各个节点的端口状态

查看环上各个节点的端口状态是否正常。

命令：*display rrpp verbose domain domain-id*

例如：通过命令查看，可以确认该节点为主节点，主端口为 Up 状态副端口为 Blocked 状态，即环网为健康状态。

```
<H3C> display rrpp verbose domain 1
Domain ID          : 1
Control VLAN       : Major4000       Sub 4001
Protected VLAN : Reference Instance 0
Hello Timer        : 1   sec    Fail Timer : 3   sec
Fast Detection Status: Disable
Fast Hello Timer: 100 ms       Fast Fail Timer: 300 ms
Ring ID            : 1
Ring Level         : 0
Node Mode          : Master
Ring State         : Complete
Enable Status      : Yes      Active Status: Yes
Primary port       : GE1/0/1                    Port status:Up
Secondary port     : GE1/0/2                    Port status:Blocked
```

（5）查看环上各个节点的协议报文收发情况

查看环上各个节点的协议报文收发情况。

命令：*display rrpp statistics domain domain-id*

例如：通过命令查看，可以确认主端口 GE1/0/1 发送了 16424 个 Hello 报文和 1 个 Complete Flush FDB 报文；副端口 GE1/0/2 接收了 16424 个 Hello 报文和 1 个 Complete Flush FDB 报文。

```
<Sysname> display rrpp statistics domain 1
Ring ID          : 1
Ring Level       : 0
Node Mode        : Master
Active Status    : Yes
Primary port     : GE1/0/1
Fast Hello Packets: 0 Send, 0 Rcv
Fast Edge Hello Packets: 0 Send, 0 Rcv
```

```
Packet             Link      Common      Complete    Edge    Major   Packet
 Direct    Hello   Down      Flush FDB   Flush FDB   Hello   Fault   Total
----------------------------------------------------------------------------
 Send      16424   0         0           1           0       0       16425
 Rcv       0       0         0           0           0       0       0
Secondary port: GE1/0/2
 Packet            Link      Common      Complete    Edge    Major   Packet
 Direct    Hello   Down      Flush FDB   Flush FDB   Hello   Fault   Total
----------------------------------------------------------------------------
 Send      0       0         0           0           0       0       0
 Rcv       16424   0         0           1           0       0       16425
```


郝云龙
IRF II 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查堆叠及MAD状态
检查成员设备是否单体故障
检查CPU占用率
检查软硬件一致性
查看IRF-Port口状态
检查IRF配置
检查IRF-Port物理连接
检查IRF报文是否超时
检查堆叠链路
拨打热线
400-810-0504寻求帮助

1. 开始

定位故障的思路是：先检查堆叠及MAD状态是否正常，再检查设备是否故障，然后检查堆叠链路，最后检查配置。

2. 流程图相关操作说明

(1) 检查堆叠及MAD状态

检查各成员设备是否正确处于堆叠状态以及MAD检测机制是否检测到分裂。

命令：*display irf*

display mad verbose

例如：通过命令查看，可以确认各成员设备已经正确处于堆叠状态，且MAD处于检测状态。

```
<H3C>display irf
Switch   Role     Priority    CPU-Mac           Description
 *+1     Master   10          c4ca-d9ab-8c95     -----
   2     Slave    1           c4ca-d9ab-8cf5     -----
-------------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: c4ca-d9ab-8c94
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
<H3C> display mad verbose
Current MAD status:Detect
Excluded ports(configurable):
  Vlan-interface999
Excluded ports(can not be configured):
  Ten-GigabitEthernet1/0/25
MAD ARP enabled interface:
  Vlan-interface2
MAD enabled aggregation port:
  Bridge-Aggregation1
MAD BFD enabled interface:
  Vlan-interface3
    mad ip address 3.3.3.1 255.255.255.0 member 1
    mad ip address 3.3.3.2 255.255.255.0 member 2
```

如果MAD当前的状态为Recovery，表示发生多Active冲突，即堆叠分裂。

(2) 检查成员设备是否单体故障

要保证堆叠系统的正常建立及运行，必须确保各成员的正常运行，检查设备及堆叠接口是否硬件故障，并检查设备的基本运行是否正常。

例如：通过查看设备面板SYS、POWER指示灯绿色常亮，7段数码指示灯（盒式设备）绿色常亮且显示具体的数字，主控板上对应堆叠接口板槽位指示灯（框式设备）RUN闪烁、ALM

灯灭，可以确认设备或堆叠接口板基本运行正常。

(3) 检查硬件、软件一致性

IRF 的正常建立对设备及软件版本有严格的要求：软件版本必须一致且硬件满足堆叠条件。

命令：*display version*

例如：通过命令查看，可以确认各成员设备软件版本一致。

```
<H3C>display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 2108P01
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S3600V2-52TP-EI uptime is 0 week, 0 day, 3 hours, 26 minutes

<H3C>dis version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 2108P01
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S3600V2-52TP-EI uptime is 0 week, 0 day, 3 hours, 32 minutes
```

(4) 查看 IRF-Port 口状态

确认堆叠口状态是否正常 Up。

命令：*display irf topology*

例如：通过命令查看，可以确认 IRF-Port 状态正常。

```
<H3C>display irf topology
                              Topology Info
 -------------------------------------------------------------------------
              IRF-Port1                   IRF-Port2
 Switch    Link      neighbor      Link      neighbor      Belong To
 1         DIS       --            Up        2             c4ca-d9ab-8c95
 2         Up        1             DIS       --            c4ca-d9ab-8c95
```

(5) 检查堆叠链路

确保堆叠链路的正常是堆叠建立的关键，包括检查专用堆叠电缆或光模块、光纤以及 IRF 物理口是否正常。

命令：*display transceiver diagnosis interface interface-type interface-number*

例如：通过命令查看光模块信息，可以确认光模块收发功率都在正常范围。

```
[H3C]display transceiver diagnosis interface GigabitEthernet 1/0/52
GigabitEthernet1/0/52 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(¡ãC)   Voltage(V)   Bias(mA)   RX power(dBm)   TX power(dBm)
    42           3.32         19.15      -4.13           -6.77
```

通过替换测试来进一步排除堆叠电缆、光模块、光纤、IRF 物理口的故障，确保 IRF 正常建立。

(6) 检查 IRF 配置

IRF 的配置是否正确。

命令：*display current-configuration*

例如：通过命令查看，可以确认 IRF 配置正确。

```
<H3C>display current-configuration
…
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 10
#
…
#
 irf-port 1/2
 port groupinterface GigabitEthernet1/0/52 mode normal
#
 irf-port 2/1
 port groupinterface GigabitEthernet2/0/52 mode normal
#
…
```

（7）检查 IRF-Port 物理连接

本设备上与 IRF-Port1 绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port2 口上绑定的 IRF 物理端口相连，本设备上与 IRF-Port2 口绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port1 口上绑定的 IRF 物理端口相连，否则不能形成 IRF。

命令：*display current-configuration*

例如：通过命令查看，成员设备 1 配置了 IRF-Port2，成员设备 2 配置了 IRF-Port1，并通过堆叠链路正确连接。

```
<H3C>display current-configuration
…
#
 irf-port 1/2
 port groupinterface Ten-GigabitEthernet1/0/52 mode normal
#
 irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/52 mode normal
#
…
```

（8）检查 IRF 报文是否超时

成员设备间是否正常交互 IRF Hello 报文。

命令：*display irf topology*

例如：通过命令查看，IRF Hello 报文超时。

```
<H3C>display irf topology
                              Topology Info
 -------------------------------------------------------------------------
                IRF-Port1                  IRF-Port2
 Switch     Link        neighbor      Link        neighbor     Belong To
 1          DIS         --            TIMEOUT     2            c4ca-d9ab-8c95
 2          TIMEOUT     1             DIS         --           c4ca-d9ab-8c95
```


王 京
Hey There
QoS故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看端口优先级配置和信任模式
查看重标记配置
查看优先级映射表和队列统计信息
修改优先级映射表
接口速率和链路带宽是否匹配
检查接口LR或GTS配置
查看队列调度配置
查看拥塞避免配置
拨打热线 400-810-0504寻求帮助

03 交换技术 › 3.5 QoS › QoS 故障排查 › 步骤详解

1. 开始

定位故障的思路是：在入端口进行流量分类，报文根据优先级进入不同队列；在出端口拥塞时，各队列采用不同的调度方式，差异化的转发报文。

先查流标记，再查优先级映射，然后查看队列调度，最后查看拥塞避免。

2. 流程图相关操作说明

（1）查看端口优先级配置和信任模式

查看流量进入交换机接口的端口优先级配置和信任模式。

命令：*display qos trust interface interface-type interface-number*

例如：通过命令查看，可以确认 GigabitEthernet 1/0/1 的端口优先级为 4，信任模式为 802.1p。设备将根据报文携带的 802.1p 优先级查找映射表进行优先级映射；而接收到的报文没有携带 802.1Q 标签时，设备将使用接收端口的端口优先级 4 作为报文的 802.1p 优先级，并依此进行优先级映射。

```
<H3C>display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority :4
  Port priority trust type :dot1p
```

（2）查看重标记配置

查看交换机端口入方向是否配置了重标记策略。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，可以确认端口 GigabitEthernet1/0/1 下发了重标记策略，对匹配 ACL3000 的报文重标记 802.1p 优先级为 5。

```
<H3C>display qos policy interface GigabitEthernet1/0/1
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: qos
   Classifier: qos
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: qos
     Marking:
        Remark dot1p COS 5
```

（3）查看优先级映射表和队列统计信息

查看设备的优先级映射表，检查报文的携带优先级是否映射到了期望的调度优先级。

命令：*display qos map-table dot1p-lp*

例如：通过命令查看，可以确认 802.1p 优先级 5 映射到了本地优先级 5。

```
<H3C>display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp    TYPE: pre-define
```

```
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

查看端口队列统计信息，检查报文匹配情况。

命令：*display qos queue-statistics interface interface-type interface-number*

例如：通过命令查看，可以确认本地优先级5队列已经有报文匹配通过。

```
<H3C>display qos queue-statistics interface GigabitEthernet 1/0/2
Interface: GigabitEthernet1/0/2
Direction: Outbound
Queue  Queued packets  Passed packets  Dropped packets  Passed rate(bps)
  0          0               0               0                0
  1          0               0               0                0
  2          0               1               0                0
  3          0               0               0                0
  4          0               0               0                0
  5          0              96               0             3000
  6          0               0               0                0
  7          0               4               0                0
```

(4) 修改优先级映射表

修改报文的携带优先级使之映射到期望的调度优先级。

命令：*qos map-table dot1p-lp*

例如：修改802.1p优先级0映射到了本地优先级1；修改802.1p优先级5映射到了本地优先级2。

```
[H3C-maptbl-dot1p-lp]dis this
#
qos map-table dot1p-lp
 import  0  export  1
 import  5  export  2
#
return
```

(5) 查看队列调度配置

查看队列调度配置，检查调度类型是否满足业务要求。

命令：*display qos sp/wrr/wfq interface interface-type interface-number*

例如：通过命令查看，可以确认接口GigabitEthernet 1/0/2使能了SP+WFQ队列，其中5队列属于SP调度组，其他队列属于WFQ调度组。

```
[H3C-GigabitEthernet1/0/2]display this
#
interface GigabitEthernet1/0/2
```

```
port link-mode bridge
 qos wfq byte-count
 qos wfq  5 group sp
#
Return
[H3C]display qos wfq interfaceGigabitEthernet1/0/2
Interface: GigabitEthernet1/0/2
 Output queue: Hardware weighted fair queue
Queue ID        Group           Byte-count       Min-Bandwidth
------------------------------------------------------------
0               1               1                64
1               1               1                64
2               1               1                64
3               1               1                64
4               1               1                64
5               sp              NA               64
6               1               1                64
7               1               1                64
```

(6) 接口速率和链路带宽是否匹配

检查接口运行速率是否等于链路带宽。

命令：*display interface interface-type interface-number*

例如：通过命令查看，可以确认接口 GigabitEthernet 1/0/2 运行速率为 100Mbps。

```
[H3C]display interface GigabitEthernet 1/0/2
------------------------------------------------------------
100Mbps-speed mode, full-duplex mode
------------------------------------------------------------
```

(7) 检查接口 LR 或 GTS 配置

查看接口是否配置了 LR 或 GTS，确保限速带宽和链路带宽一致。

命令：*display qos lr/gts interface interface-type interface-number*

例如：通过命令查看，可以确认接口 GigabitEthernet1/0/2 配置了 LR 限速，出方向带宽限速为 10Mbps。

```
[H3C]display qos lr interface GigabitEthernet1/0/2
Interface: GigabitEthernet1/0/2
Direction: Outbound
 CIR  10240 (kbps),   CBS 640000 (byte)
```

(8) 查看拥塞避免配置

查看接口是否应用了 WRED，以及 WRED 表的配置情况。

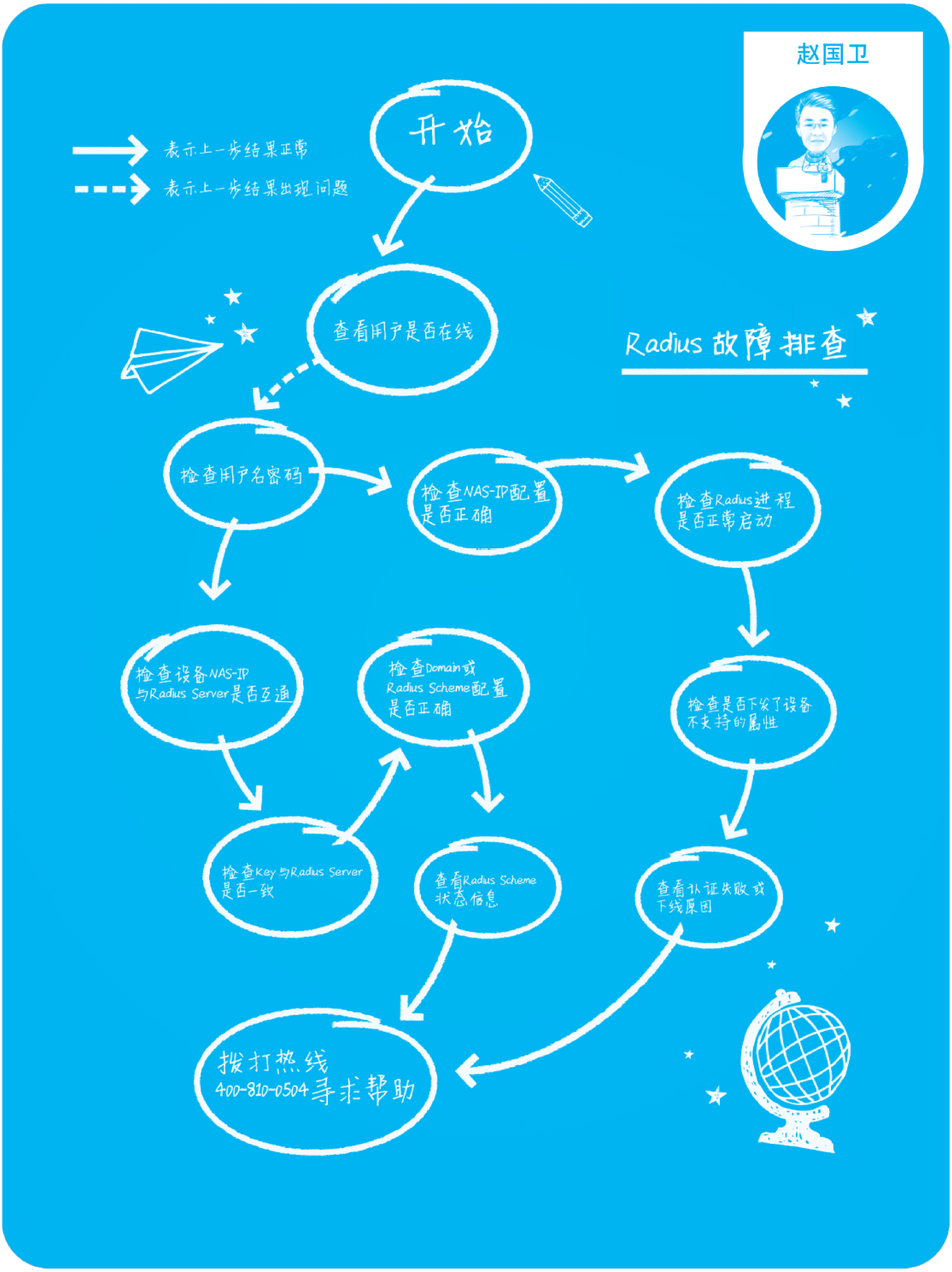
命令：display qos wred interface *interface-type interface-number*；display qos wred table *interface-type interface-number*

例如：通过命令查看，可以确认 GigabitEthernet1/0/2 口已应用了 WRED。在 WRED 表的参数配置中，队列 5 的丢弃概率为 0，其他队列的丢弃概率采用设备默认值。

```
[H3C]display qos wred interfaceGigabitEthernet1/0/2
Interface: GigabitEthernet1/0/2
 Current WRED configuration:
```

```
Applied WRED table name: 1

[H3C]display qos wred table
Table Name: 1
Table Type: Queue based WRED
QID: gmin   gmax   gprob   ymin   ymax   yprob   rmin   rmax   rprob exponent   ecn
--------------------------------------------------------------------------------------
 0    100   1000   10      100    1000   10      100    1000   10       9        N
 1    100   1000   10      100    1000   10      100    1000   10       9        N
 2    100   1000   10      100    1000   10      100    1000   10       9        N
 3    100   1000   10      100    1000   10      100    1000   10       9        N
 4    100   1000   10      100    1000   10      100    1000   10       9        N
 5    100   1000   0       100    1000   0       100    1000   0        9        N
 6    100   1000   10      100    1000   10      100    1000   10       9        N
 7    100   1000   10      100    1000   10      100    1000   10       9        N
```


赵国卫
表示上一步结果正常
表示上一步结果出现问题
开始
查看用户是否在线
Radius 故障排查
检查用户名密码
检查NAS-IP配置是否正确
检查Radius进程是否正常启动
检查设备NAS-IP与Radius Server是否互通
检查Domain或Radius Scheme配置是否正确
检查是否下发了设备不支持的属性
检查Key与Radius Server是否一致
查看Radius Scheme状态信息
查看认证失败或下线原因
拨打热线
400-810-0504寻求帮助

1．开始

Radius 协议承载于 UDP 协议，是基于 C/S 架构的，客户端和服务器都要排查。所以定位故障的思路是分别检查作为 Radius 客户端的设备侧和 Radius 服务器。

2．流程图相关操作说明

（1）查看用户是否在线

在设备上查看用户是否在线。

命令：*display connection*

display connection ucibindex ucibindex-number

例如：通过命令查看在线用户信息，可以确认用户名 admin 的用户已经在线，其用户索引为 134，后面跟 ucibindex 参数及对应用户的索引 134 可查看对应在线用户 admin 的详细信息。

```
<H3C>display connection
Slot:  1
Index=134 , Username=admin@system
 IP=10.153.47.44
 IPv6=N/A
<H3C>display connection ucibindex 134
Slot:  1
Index=134, Username=admin@system
IP=10.153.47.44
IPv6=N/A
Access=Admin    ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
Initial VLAN=N/A, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2013-05-06 14:08:43 ,Current=2013-05-06 14:50:47 ,Online=00h42m04s
 Total 1 connection matched.
```

（2）检查用户名密码

确保客户端输入的用户名密码正确。

（3）检查设备 NAS-IP 与 Radius Server 是否互通

确保设备到 Radius ServerIP 地址和端口可达。

（4）检查 Key 与 Radius Server 是否一致

查看设备侧配置的 Radius Key 和 Radius Server 侧配置的 Key 是否一致。

命令：*display this*

例如：通过命令查看 Key 配置。

```
[H3C]radius scheme imc
[H3C-radius-imc]display this
```

```
radius scheme imc
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 key authentication h3c
 key accounting h3c
 user-name-format without-domain
```

(5) 检查 Domain 或 Radius Scheme 配置是否正确

如果设备要做 EAD 或者下发 H3C 私有 Radius 属性，则需要将服务类型配置为 extended。

命令：*display this*

例如：Radius Scheme 视图下查看服务类型是否为 extended。

```
[H3C-radius-imc]display this
server-type extended
 primary authentication 1.1.1.1
 primary accounting 1.1.1.1
 secondary authentication 1.1.1.17
 secondary accounting 1.1.1.17
```

我们设备默认的 domain 域是 system，如果不指定域后缀，用户认证的时候都会到默认的 system 域去认证，要检查默认域是否配置为用户的认证域。另外不管是否存在计费和授权，在 domain 下都要同时指定认证、授权、计费的 Radius-scheme，三者同配，缺一不可。

命令：*display this*

domain default enable h3c

例如：查看配置中认证、授权、计费的引用，并配置用户认证域 H3C 为默认的 domain。

```
[H3C]domain h3c
[H3C-isp-h3c]display this
#
domain h3c
 authentication default radius-scheme imc
 authorization default radius-scheme imc
 accounting default radius-scheme imc
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable

[H3C]domain default enable h3c
```

(6) 查看 Radius Scheme 状态信息

不仅仅要确认到 Radius 服务器路由可达，还要确认对应认证、计费、授权服务器是否端口可达。

命令：*display raidus scheme*

例如：通过命令查看 radius scheme 状态信息，确认其状态为 Active。

```
<H3C>display radius scheme imc
SchemeName   : imc
  Index : 1                          Type : extended
  Primary Auth Server:
    IP: 1.1.1.1                           Port: 1812    State: active
    Encryption Key : N/A
    VPN instance   : N/A
    Probe username : N/A
    Probe interval : N/A
  Primary Acct Server:
    IP: 1.1.1.1                           Port: 1813    State: active
    Encryption Key : N/A
    VPN instance   : N/A
```

(7) NAS-IP 配置是否正确

检查服务器侧是否配置了 NAS-IP 以及配置的 NAS-IP 是否与设备指定的 NAS-IP 一致。

如图 3-5 所示，这里设备的 NAS-IP 为 10.1.1.200，则在 iMC 侧配置的接入设备 IP 也要是 10.1.1.200。



图 3-5 查看设备移入配置信息

(8) Radius 进程是否正常启动

查看服务器侧 Radius 进程是否正常启动，是否存在应用端口号被占用的情况，以及是否配置 Radius 代理。

(9) 是否下发了设备不支持的属性

服务器可以下发各种 Radius 属性，有些属性对格式有要求，要注意下发的属性格式在设备上是否能够支持。如果下发了设备不支持的属性会导致认证失败。常用的 Radius 属性有：

用户权限、ACL、VLAN、CAR 限速。常见的 Radius 属性如表 3-2 所示。

表 3-2 常见 Radius 属性

属性名	属性编号	格式(Text,String,Address,Integer)	具体定义
Input-Peak-Rate	1	Integer	用户接入到 NAS 的峰值速率,以 bps 为单位
Input-Average-Rate	2	Integer	用户接入到 NAS 的平均速率,以 bps 为单位
Input-Basic-Rate	3	Integer	用户接入到 NAS 的基本速率,以 bps 为单位。(这个域目前没有意义,建议不要使用)
Output-Peak-Rate	4	Integer	从 NAS 到用户的峰值速率,以 bps 为单位
Output-Average-Rate	5	Integer	从 NAS 到用户的平均速率,以 bps 为单位
Output-Basic-Rate	6	Integer	从 NAS 到用户的基本速率,以 bps 为单位。(这个域目前没有意义,建议不要使用)
Exec-Privilege	29	Integer	EXEC 用户优先级。 对于 EXEC 用户,用户的优先级。用来设置 EXEC 用户的优先级。RADIUS 服务器在认证接收报文中,可以用属性 Exec_Privilege 携带 EXEC 用户的优先级。该属性是针对管理用户的设置
Tunnel-Private-Group-ID	81	Integer	参照 RFC 定义,用作 VPDN 组号。 说明:为了与以前设备实现的方式兼容,该属性取值为[1-4094]下发给设备的值的类型为 Integer,其他值的类型为 String
Tunnel-Assignment-ID	82	Integer	参照 RFC 定义
Filter-ID	11	String (协议中规定此属性类型为 Text)	访问控制列表的名字。不同产品实现定义不同。建议客户端不要对 RADIUS 服务器上定义的 Filter-Id 的名字做限制,具体的规则在客户端上进行配置 MA5200:ACLGroup@InterGroup,其中 ACLGroup 可以是 ACL 组号,也可以为是 ACL 组名;InterGroup 及既可以是 InterGroup 组号,也可以是 InterGroup 组名。如果带有多个 Filter-ID,则只有最后一个 Filter-ID 起作用,因此建议只带一个 Filter-ID

(10) 查看认证失败或下线原因

Radius 服务器都会有对应的日志记录用户认证失败或下线的原因。常见的下线原因,可以参考下面的说明。

```
Acct-Terminate-Cause     User-Request          1
```

#这种情况,属于用户请求下线,一般为客户端主动下线,需要检查客户端。

```
Acct-Terminate-Cause     Lost-Carrier         2
```

#这种情况一般为客户端与设备间握手报文丢失导致,因为 H3C 设备的握手功能是私有的,在跟第三方客户端配合时,需要关闭握手。

关闭握手的命令为:*undo dot1x handshake*

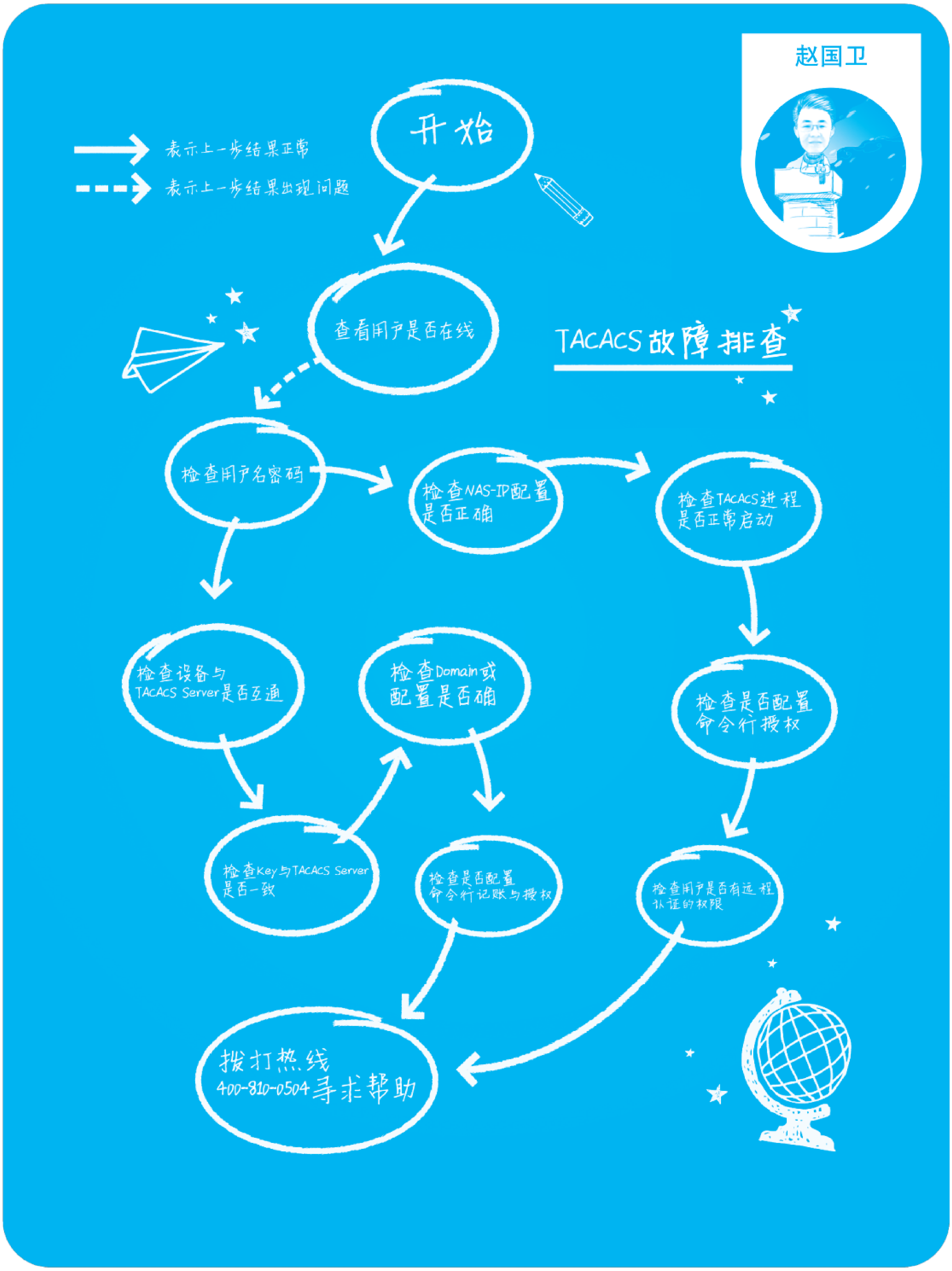
例如:关闭端口 G1/0/10 下的 dot1x 握手功能。

```
[H3C]int g1/0/10
[H3C-GigabitEthernet1/0/10]undo dot1x handshake
Acct-Terminate-Cause      Idle-Timeout            4
```

#这种情况为闲置超时下线。

```
Acct-Terminate-Cause      Session-Timeout         5
```

#这种情况为会话超时，一般为计费不足或者进行了时间段限制。



赵国卫
表示上一步结果正常
表示上一步结果出现问题
开始
查看用户是否在线
TACACS 故障排查
检查用户名密码
检查NAS-IP配置是否正确
检查TACACS进程是否正常启动
检查设备与TACACS Server是否互通
检查Domain或配置是否确
检查是否配置命令行授权
检查Key与TACACS Server是否一致
检查是否配置命令行记账与授权
检查用户是否有远程认证的权限
拨打热线 400-810-0504寻求帮助

1. 开始

TACACS 协议是基于 C/S 架构承载于 TCP 之上，客户端和服务器都要排查。所以定位故障的思路是分别检查作为 TACACS 客户端的设备侧和 TACACS 服务器。

2. 流程图相关操作说明

(1) 查看用户是否在线

在设备上查看用户是否在线。

命令：*display connection*

display connection ucibindex ucibindex-number

例如：通过命令查看 admin 用户已经在线，其用户索引为 134 后面跟 ucibindex 参数及对应用户的索引 134 可查看对应在线用户 admin 的详细信息。

```
<H3C>display connection
Slot:  1
Index=134 , Username=admin@system
 IP=10.153.47.44
 IPv6=N/A
<H3C>display connection ucibindex 134
Slot:  1
Index=134 , Username=admin@system
IP=10.153.47.44
IPv6=N/A
Access=Admin    ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
Initial VLAN=N/A, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
SessionTimeout=N/A, Terminate-Action=N/A
Start=2013-05-06 14:08:43 ,Current=2013-05-06 14:50:47 ,Online=00h42m04s
 Total 1 connection matched.
```

(2) 检查用户名密码

检查输入的用户名密码是否正确。

(3) 检查设备与 TACACS Server 是否互通

确保设备与 TACACS Server 之间 IP 和端口可达。

(4) 检查 Key 与 TACACS Server 是否一致

查看设备侧配置的 TACACS Key 和 TACACS Server 侧配置的 Key 是否一致。

命令：*display this*

例如：通过命令查看 Key 配置，这里配置的 Key 是 h3c，在 server 侧也要配置一样的 Key。

```
[H3C]hwtacacs scheme Tacacs
[H3C-hwtacacs-acs]display this
```

```
primary authentication 1.1.1.1
primary authorization 1.1.1.1
primary accounting 1.1.1.1
key authentication h3c
key authorization h3c
key accounting h3c
user-name-format without-domain
```

（5）检查 Domain 域配置是否正确

H3C 设备默认的 domain 域是 system，如果不指定域后缀，用户认证的时候都会到默认的 system 域去认证，要检查默认域是否配置为用户的认证域，另外不管是否存在计费和授权，在 domain 下都要同时指定认证、授权、计费的 hwtacacs-scheme，否则默认都走本地容易导致认证失败。

命令：*domain default enable*

例如：查看配置中认证、授权、计费的引用的 TACACS Scheme 是 Tacacs，并配置用户认证域 H3C 为默认的 domain。

```
[H3C]domainH3C
[H3C-isp-H3C]display this
domainH3C
 authentication login hwtacacs-scheme Tacacs
 authorization login hwtacacs-scheme  Tacacs
 accounting login hwtacacs-scheme  Tacacs
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
[H3C]domain default enable H3C
```

（6）检查是否配置命令行记账与授权

如果要对用户进行命令行授权和记账则需要在 vty 接口下添加相应配置。

命令：*command authorization*

command accounting

例如：对 user-interface vty 0～4 配置命令行授权与记账功能。

```
[H3C]user-interface vty 0 4
 authentication-mode scheme
 command authorization
 command accounting
 idle-timeout 120 0
 screen-length 30
```

（7）检查 NAS-IP 配置是否正确

NAS-IP 是设备和服务器进行通信的 IP 地址，服务器会对 NAS-IP 进行检查确定是否是合法的 NAS 设备。要检查 TACACS 服务器侧是否配置了 NAS-IP 以及配置的 NAS-IP 是否与设备侧指定的 NAS-IP 一致。

（8）检查 TACACS 进程是否正常启动

查看服务器侧 TACACS 进程是否正常启动，是否存在应用端口号被占用的情况。

TACACS 默认使用的认证、授权、计费端口号都是 TCP 49。

(9) 检查是否配置命令行授权

检查命令行授权配置格式是否正确。

(10) 检查用户是否有远程认证的权限

确认在服务器上已经建立了相应的认证用户，并且赋予了用户远程认证权限。

04

路由器产品

陈丹威



MSR G2设备License异常故障排查



1. 开始

MSR G2 系列路由器是搭载了 H3C 自主研发的 Comware V7 平台的新一代开放多业务路由器产品，其启动文件可以分为基本软件包和特性软件包。若用户只有一些基本的业务需求，则设备仅需要加载基本软件包即可；但若客户需要使用一些高级特性，例如 MPLS、语音等，则需要购买对应的软件授权函，成功激活后才可以在设备上加载特性软件包，满足客户的特性需求。

MSR G2 路由器的 License 和设备一一对应，设备 License 异常的定位故障的思路是：首先确认 License 能否正常激活，查看激活文件是否正确，再看当前 License 的使用状态是否正常，最后判断特性软件包是否已经正常加载。

2. 流程图相关操作说明

(1) License 能否正常激活

客户使用软件授权函在官网完成 License 的激活之后会获得一个扩展名为 ak 的激活文件。建议使用 TFTP 将激活文件上传到设备上，然后执行命令进行 License 激活操作。

正常情况下，License 可以被激活。但是如果激活文件有问题，就无法完成激活操作。

命令：*license activation-file install file-name*

例如：使用激活文件激活 License 时，正常情况下会激活并成功安装特性软件包；若激活文件有问题，则会提示激活失败。

```
[H3C]license activation-file install 210231A1UYB13300003220130533000.ak
[H3C]%May 31 15:07:54:394 2014 H3C PKG/5/PKG: Installing package cfa0:/msr56-cmw710-data-R0106.bin on slot 0...
%May 31 15:07:57:098 2014 H3C PKG/5/PKG: cfa0:/msr56-cmw710-data-R0106.bin installed on slot 0.

[H3C]license activation-file install cfa0:/210235A0W8B1380003280404190.ak
Failed to install the activation file.
```

(2) 确认激活文件是否正确

在使用扩展名为 ak 的激活文件执行激活操作时，若无法正常激活 License 就一定是激活文件有问题。

激活文件异常只有两种可能：激活文件注册有误或激活文件被损坏。

在客户购买设备较多时，每台设备分别注册激活文件，可能会将一台设备的 SN 和另一台设备的 DID 混在一起注册激活文件，就导致了文件注册时出错。由于 MSR G2 设备的激活文件和设备一一对应，必须是同一台设备的 SN 和 DID 注册生成的激活文件，才可以用于激活该设备的特性软件包。可以通过命令查看激活文件中的设备信息是否和注册的设备一致，若信息有误，需进行 License 的解绑定操作，解绑之后再重新注册。

激活文件损坏，可能是传输异常或人为操作导致的。

Comware V7 平台是基于 Linux 内核的系统，由于 Windows 和 Linux 系统 ASCⅡ 编码方式对字符的定义有差别，在使用 FTP 的 ASCⅡ 模式向 MSR G2 路由器传输文件时，会导致文件的内容损坏。建议使用 TFTP 进行文件传输，也可以使用 FTP 的二进制模式传输文件。

License 激活文件必须是 H3C 官网下发的扩展名为 ak 的原文件，若用户对激活文件的内容进行过编辑，也会导致激活文件不可用。

命令：*more file-url*

display license device-id

license activation-file uninstall file-name

例如：可以通过 more 命令查看激活文件的内容，若其中的设备信息与 display license device-id 显示的不完全一致，则需要进行激活文件的解绑定操作。

```
<H3C>more 210235A0W3B1330000972013042408525130572.ak
…
------------------------- License data -------------------------
Type                        : 00010002
SN                          : 210235A0W8B138000507
Device ID                   : Fnk@-#EEN-vCkK-Sg/Q-7%XW-MvCL-djfJ-Th5H
…
<H3C>display license device-id
SN:210235A0W8B138000507
Device ID: Z:SL-AG%k-7cbC-Y6Tp-9sxW-wEc:-3mRd-a3$8
[H3C]license activation-file uninstall20142394823.ak
Uninstall file: flash:/license/20142394823.uak
```

(3) 重新上传或申请激活文件

若是由于客户上传了编辑过的激活文件或是使用 FTP 的 ASCⅡ模式传输的激活文件，导致激活文件错误而无法激活，此时只需要保证使用 H3C 官网下发的原文件，并使用 TFTP 再次上传文件，即可正常的完成激活操作。

若是激活文件注册有误，则必须进行 License 的解绑定操作，解绑之后在官网进行从新注册。License 的解绑定需由 H3C 的工程师提交工作联络单来完成，客户需要说明解除绑定的原因，提供激活成功的文件、授权序列号、最终用户单位名称、条码等信息。

命令：*tftp tftp-server get source-filename*

license activation-file install file-name

例如：使用 TFTP 上传扩展名为 ak 的激活文件，完成 License 的激活操作，并成功加载特性软件包。

```
<H3C>tftp 1.1.1.2 get 210231A1UYB1330000322013053114203000.ak
%   Total   % Received % Xferd Average  Speed   Time     Time     Time     Current
                               Dload    Upload  Total    Spent    Left     Speed
100  2296 100  2296     0    0  25421    0      --:--:-- --:--:-- --:--:-- 280k
[H3C]license activation-file install 210231A1UYB1330000322013053114203000.ak
[H3C]%May 31 15:07:54:394 2014 H3C PKG/5/PKG: Installing package cfa0:/msr56-cmw710-data-R0106.bin on slot 0...
%May 31 15:07:57:098 2014 H3C PKG/5/PKG: cfa0:/msr56-cmw710-data-R0106.bin installed on slot 0.
```

(4) 查看当前 License 是否 In use 状态

若设备的 License 能够正常激活，那么 License 的使用状态应该是 In use，只有这种状态下特性软件包才会被加载。

命令：*display license*

例如：查看当前设备上的 License 状态，In use 是正常状态。

```
<H3C>display license
cfa0:/license/210235A0WAA12900000120121024123492348 36.ak
Feature: pkg_license
Product Description: H3C MSR36 Data Software License
Registered at: 2013-05-09 08:41:12
License Type: Permanent Current State: In use
```

(5) License 状态显示 Uninstalled 或 Expired

激活文件在被客户手动卸载之后，License 的当前状态就会显示为 Uninstalled。

MSR G2 路由器的 License 不能随意卸载，因为卸载之后该激活文件便失效。卸载后的激活文件在该设备上再安装时，会提示该文件已被卸载"The activation file has been uninstalled."。必须进行解绑定操作后，才可以在官网重新进行注册。

卸载设备上的激活文件后，会生成一个 uninstall Key 用于解绑定。License 的解绑定需由 H3C 的工程师提交工作联络单来完成，客户需要说明解除绑定的原因，提供激活成功的文件、授权序列号、最终用户单位名称、条码等信息。

在一些特殊的场景下，客户可能会使用试用版的 License。试用版的 License 都有一定的使用期限，在试用版的激活文件到期后，License 的当前状态就会显示为超期 Expired。显示超期的激活文件将不会生效，无法正常地加载对应的特性软件包。超期后的试用版激活文件将作废，无法解绑定也不可能再给任何设备使用。

若一台设备上有多个针对某一软件特性包的激活文件，只要其中有一个处于 In use 的状态，该特性软件包就会被加载，其余已卸载或超期的激活文件对软件包的正常加载没有任何影响。

命令：*display license*

例如：查看当前设备上的 License 状态，已卸载和超期的 License 均无效。只有 License 类型为 Trial(试用版)的才可能超期。

```
<H3C>display license
cfa0:/license/210235A0W8B13B000404201401221320445 1968.ak
Feature: pkg_license
Product Description: H3C MSR 36 Data Software License
Registered at: 2014-01-22 13:45:00
License Type: Permanent
Current State: Uninstalled
Uninstall Key: /y%j-/J>+-Uzer-pAhC-JY8T-H5Ev-GN@d-yUQy
Uninstall Date: 2014-01-22 13:45:46

cfa0:/license/210235A0WAA12900000120121024160546374 74.ak
Feature: pkg_license
Product Description: H3C MSR36 Voice Software License
Registered at: 2013-10-22 08:41:12
License Type: Trial (date restricted)
Trial Validity Period: 2013-10-22 to 2013-12-21
Current State:Expired
```

(6) 查看特性软件包是否加载

在设备被格式化后，通过命令 display license 查看到的 License 状态同样会是 In use。但

是在“display license”下的“Feature”和“Product Description”项中不会有描述信息，显示为“-”，说明 License 表项对应的文件已丢失或者损坏。

这是因为设备中存储的扩展名为.ak 的激活文件实际已经不存在了，当前状态中显示的“使用中”信息其实也只是假象。由于激活文件的缺失，License 实际是未激活的状态，特性软件包自然也不可能被加载。此时需要工程师将之前保存的对应该设备的激活文件重新上传到设备上，并将文件 copy 到设备的 License 文件夹内，文件名必须和“display license”中显示的名字完全一致，之后设备可以自动识别文件，完成激活文件的加载。

但是由于此过程并非执行了安装激活文件的操作，因此特性软件包无法一起加载，需要由工程师手动来加载软件包，其操作过程详见步骤(7)。

另外，在很偶然的情况下，也可能会出现扩展名为 ak 的激活文件已经被成功注册到设备上，并且使用状态显示为 In use，但是相应的特性软件包却并没有被正常加载。这时也需要工程师来手动完成加载相应特性软件包的工作。

命令：*display license*

displayinstall active

例如：通过命令查看设备当前 License 的使用状态为 In use，但只加载了基本软件包，未加载对应的数据版特性软件包。

```
<H3C>display license
cfa0:/license/210235A0WAA1290000012012102412349234836.ak
Feature: pkg_license
Product Description: H3C MSR36 Data Software License
Registered at: 2013-05-09 08:41:12
License Type: Permanent
Current State: In use
<H3C>display install active
Active packages on the device:
  cfa0:/msr36-cmw710-boot-r0106.bin
  cfa0:/msr36-cmw710-system-r0106.bin
```

(7) 手动加载软件包

在 License 状态显示为 In use，但是对应的特性软件包并未加载的情况下，需要工程师手动完成软件包的加载工作。

首先通过 install 命令手动加载特性软件包，然后 return、quit 退出命令行，之后再次通过命令行登录设备时，特性软件包就会被加载，其中支持的特性已经可以正常使用。最后切记要执行 *install commit* 命令，确认此次的安装操作。只有这样，在设备重启之后，仍会继续加载此次手动安装的特性软件包。

命令：*install activate feature file-name*

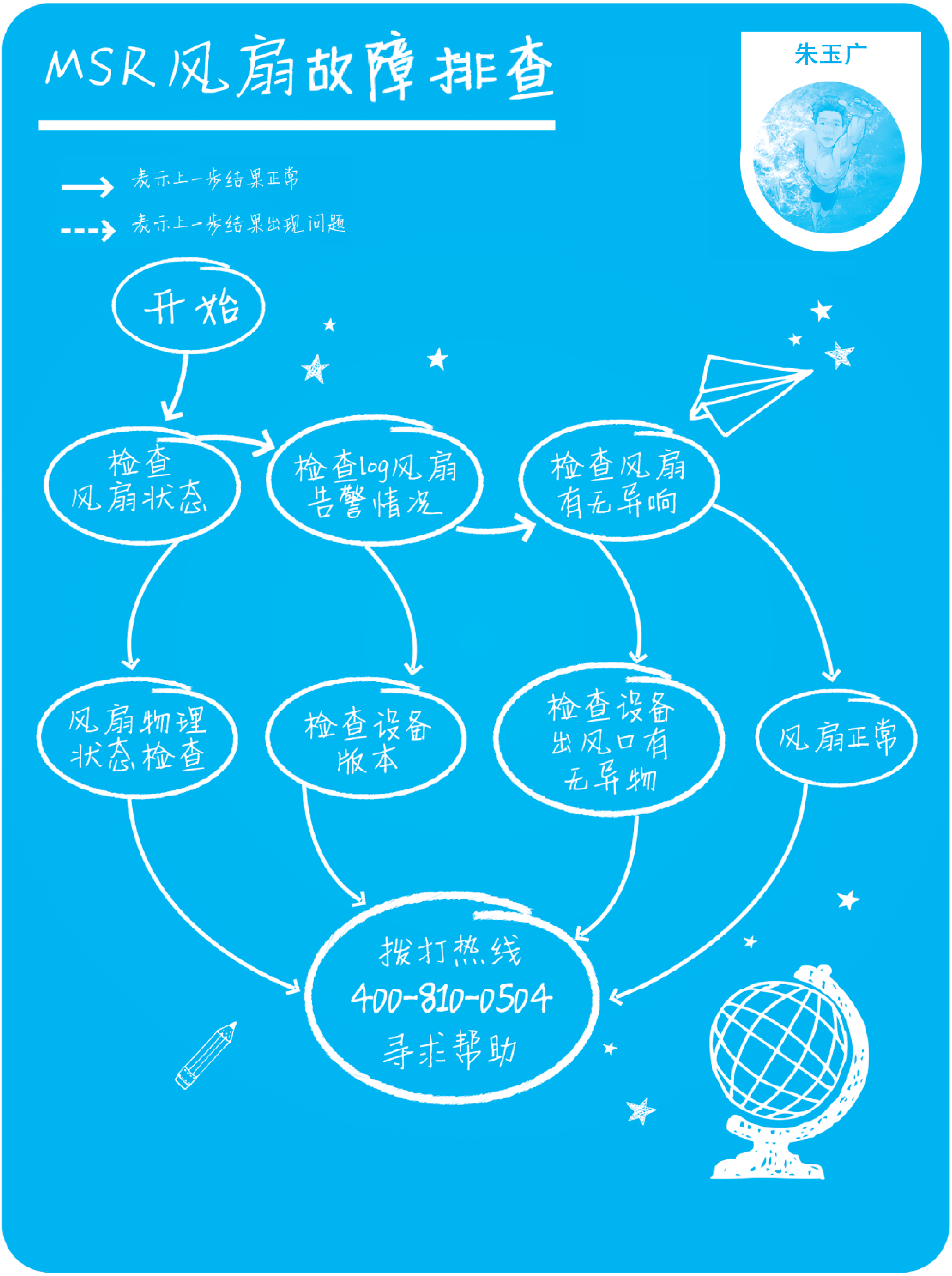
display install active

install commit

例如：手动加载特性软件包，并查看该软件包已被正常安装，之后确认此次安装操作。

```
<H3C>install activate feature cfa0:/msr36-cmw710-data-R0106.bin
Upgrade summary according to following table:
cfa0:/msr36-cmw710-data-R0106.bin
Running Version New Version
```

```
NoneRelease 0106
Upgrade Way: Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation maybe take several minutes, please wait.Done.
<H3C>display install active
Active packages on the device:
cfa0:/msr36-cmw710-boot-R0106.bin
cfa0:/msr36-cmw710-system-R0106.bin
cfa0:/msr36-cmw710-data-R0106.bin
<H3C>install commit
```


MSR风扇故障排查
朱玉广
表示上一步结果正常
表示上一步结果出现问题
开始
检查风扇状态
检查log风扇告警情况
检查风扇有无异响
风扇物理状态检查
检查设备版本
检查设备出风口有无异物
风扇正常
拨打热线
400-810-0504
寻求帮助

1. 开始

风扇是设备的重要组成部分,对于设备的正常工作起着不可或缺的作用。风扇转速由主控板控制,转速的调整范围在 50%~100%之间。风扇控制器设置了低温门限和高温门限两个参数,高温门限对应 100%的风扇转速,低温门限对应 50%的风扇转速。风扇停转时可以发出停转告警信号,任意一路风扇告警均能响应。MSR 出现风扇故障,如果所处环境散热不好,可能会出现设备由于温度过高导致运行异常的情况。MSR 风扇故障排错的定位思路是:查看风扇状态,查看 log 中风扇告警情况,检查设备版本,检查风扇有无异响,检查出风口有无异常。

2. 流程图相关操作说明

(1) 检查风扇状态

首先检查风扇的当前状态。

命令:*display fan*

例如:通过命令检查设备风扇的状态。

MSR V5 设备:

```
[H3C]display fan
 Fan    1 State: Normal
```

MSR V7 设备:

```
[H3C]display fan
Index      Status      Speedlevel
 -----------------------------
 1          Normal       1
```

在设备风扇正常的情况下,风扇的 state 或者 status 应为 Normal,当出现异常的时候,可能会出现 abnormal 或者 absent 状态。

然后可通过直观观察风扇指示灯的闪亮情况,来判定风扇状态。正常情况风扇指示灯应该为常绿,不同风扇运行情况,指示灯的状态如表 4-1 所示。

表 4-1 指示灯状态

FAN	灭	风扇不在位
	常绿	正常工作
	黄色	风扇故障

(2) 风扇物理状态检查

直观地观察风扇是否在位,通过插拔风扇,测试风扇是否接触正常。

(3) 检查 log 风扇告警情况

有些风扇问题,可能会出现时好时坏的情况,这时候在 log 信息中会有记录,检查风扇的 log 告警信息。

命令：*display logbuffer*

例如：MSR V5 设备，通过该命令检查设备风扇的告警信息，当风扇不在位时，告警如下。

```
[H3C] display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 15

%Nov 24 15:53:26:950 2014 H3C SHELL/6/SHELL_CMD: -Task=co0-IPAddr=**-User=**;
Command is display fan
%Nov 24 15:53:34:220 2014 H3C DEVM/3/FAN_ABSENT: Fan 1 is absent.
```

另外在 MSR V5 设备上还可以查看风扇 trap 告警信息。

命令：*display trapbuffer*

例如：当风扇异常时，通过该命令检查风扇 trap 告警，可以看到风扇状态变为失败的 trap 信息。

```
[H3C] display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 9

#Nov 24 15:52:34:343 2014 H3C SHELL/4/LOGIN:
 Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogIn>: login from Console
```

```
#Nov 24 15:53:34:220 2014 H3C DEVM/1/FAN STATE CHANGES TO FAILURE:
 Trap 1.3.6.1.4.1.25506.8.35.12.1.6<hh3cfanfailure>: fan ID is 1
```

当设备为 V7 设备时，可以通过如下命令查看风扇告警信息。

命令：*display logbuffer*

例如：当风扇异常时，利用该命令查看 log 中风扇信息，会有“Fan 1 failed”告警信息。

```
[H3C]display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 11

%Oct 23 18:52:47:372 2013 BY0300-HR3610-A IFNET/3/PHY_UPDOWN: Aux0 link status is up.
%Oct 23 18:54:07:113 2013 BY0300-HR3610-A DEV/2/FAN_FAILED: Fan 1 failed.
```

(4) 检查设备版本

当设备较陈旧时，可能会出现误检的情况，此时建议升级一下设备版本再进行观察。

查看设备版本。

命令：*display version*

例如：MSR56 双主控，在 R0106P11 之前版本，当热插拔主用主控的时候，会导致风扇信息同步失败而出现误检的情况，查看版本信息如下。

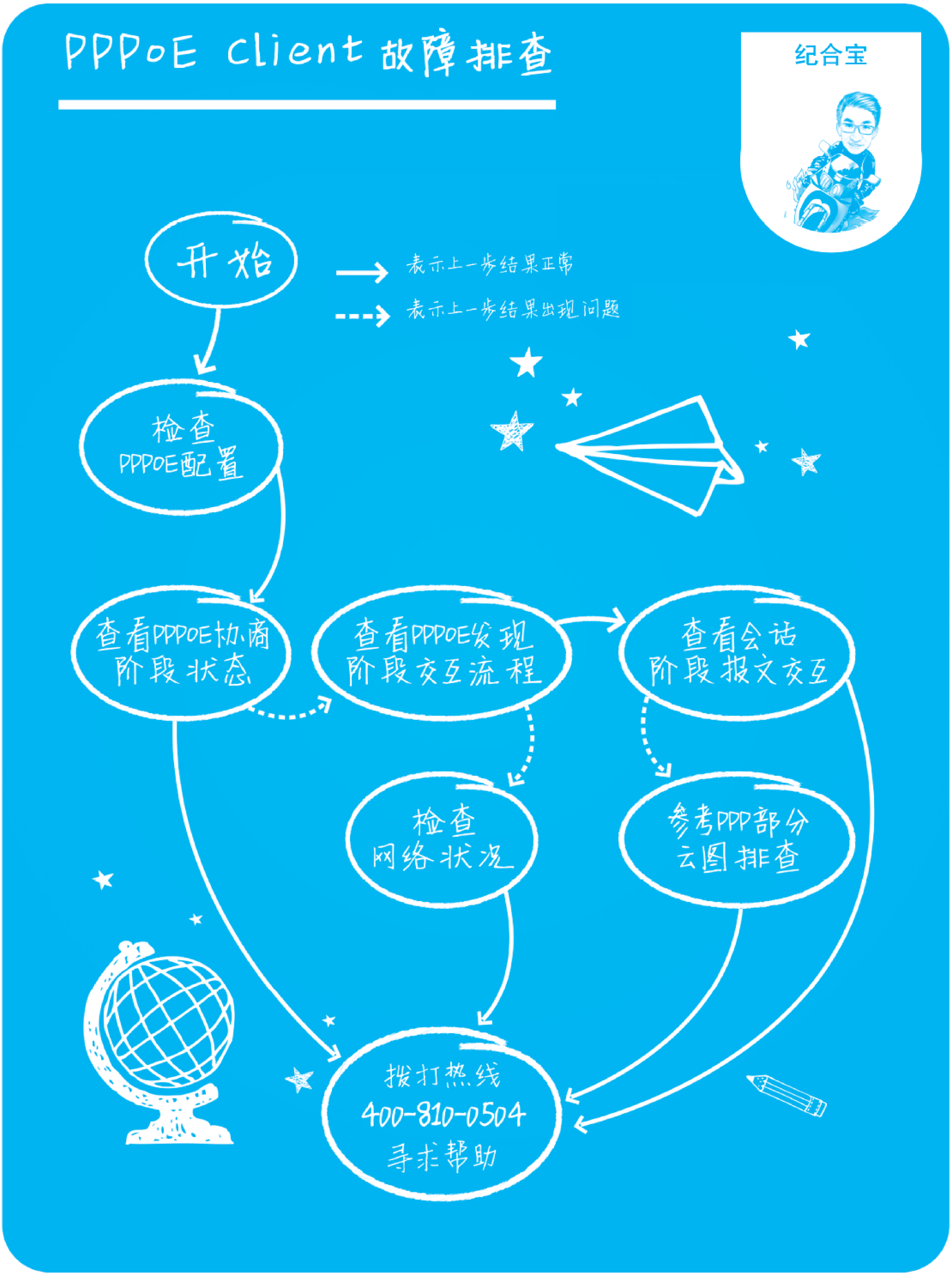
```
[H3C]display version
H3C Comware Software, Version 7.1.049, ESS 0104
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C MSR56-60 uptime is 16 weeks, 2 days, 21 hours, 29 minutes
Last reboot reason : Power on
```

(5) 检查风扇有无异响

可以直观地通过观察风扇扇叶有无转动，是否处于无障碍运行状态，然后可以用手放置到风扇处，用手感知有没有风，正常情况下，可以看到风扇转动，用手可以感知到风。

(6) 检查设备出风口有无异物

可通过直接观察风扇出风口有无障碍物异物阻挡，如果有则建议清理。


PPPoE Client 故障排查
纪合宝
开始
表示上一步结果正常
表示上一步结果出现问题
检查
PPPoE配置
查看PPPoE协商
阶段状态
查看PPPoE发现
阶段交互流程
查看会话
阶段报文交互
检查
网络状况
参考PPP部分
云图排查
拨打热线
400-810-0504
寻求帮助

1. 开始

PPPoE(Point-to-Point Protocol over Ethernet,在以太网上承载 PPP 协议)的提出,解决了 PPP 无法应用于以太网的问题,是对 PPP 的扩展。PPPoE 将 PPP 报文封装在以太网帧之内,在以太网上提供点对点的连接。PPPoE 可以通过一个远端接入设备为以太网上的主机提供互联网接入服务,并对接入的每个主机实现控制、计费功能。

PPPoE 定位故障的思路是:先查看配置是否正确,之后根据协商阶段查看 Discovery 发现阶段与 Session 会话阶段报文交互过程。

2. 流程图相关操作说明

(1) 检查 PPPoE 配置

检查配置应关注,感兴趣流是否匹配可以触发拨号,以太网口与 Dialer 拨号口是否进行关联,PPP 验证与 IP 地址分配是否正确。

命令:*display current-configuration*

例如:在设备上通过 display current-configuration 查看配置是否正确。

```
[H3C]display current-configuration
#
interface Dialer1                                  //创建拨号口
 link-protocol ppp
 ppp pap local-user 123 password simple 123        //配置 PPP 认证用户名与密码
 ip address ppp-negotiate                          //配置 IP 地址
 dialer user 123                                   //配置拨号用户名
 dialer-group 1                                    //配置拨号组与触发条件绑定
 dialer bundle 1                                   //配置 Dialer bundle
#
interface Ethernet0/0
 port link-mode route
 pppoe-client dial-bundle-number 1             //建议 PPPoE 会话,并且指定该会话所对应的 Dialer bundle
#
dialer-rule 1 ip permit                        //配置触发条件
#
```

(2) 查看 PPPoE 协商阶段状态

查看 PPPoE 协商阶段是否完成,正常状态下 State 应该为 PPPUP 状态,PPPUP 状态为 session 阶段 PPP 协商已经通过,可以传输网络数据,如果为 IDLE 则为空闲状态,没有开始 PPPoE 呼叫,PADI 则为发出 Padi 报文等待 Pado 报文,PADR 则为发出 Padr 报文等待 Pads 报文,PPPNEG 则为开始 session 阶段的 PPP 协商,如果会话状态不是 PPPUP,则需要通过 debugging pppoe-client all 命令检查报文交互信息。

命令:*display pppoe-client session summary*

例如:通过命令查看 pppoe-client 会话状态为 PPPUP。

```
<H3C>display pppoe-client session summary
PPPoE Client Session:
```

```
ID    Bundle   Dialer   Intf        RemMAC          LocMAC          State
1     1        1        Eth0/0      0023892fa780    5866ba830f70    PPPUP
```

(3) 查看 PPPoE 发现阶段交互流程

PPPoE 建立过程分为两个阶段：发现阶段(PPPoE Discovery Stage)和会话阶段(PPPoE Session Stage)，发现阶段获得对端的以太网 MAC 地址并确定一个 PPPoE SESSION_ID。

① PADI 用于 PPPoE client 发现 PPPoE 集中服务器，在 VLAN 内广播。

② PADO 用于集中服务器响应收到的 PADI 报文，声明自己能为 PPPoE client 提供服务。

③ PADR 用于 PPPoE client 向特定的 PPPoE 集中服务器申请 PPPoE 服务。

④ PADS 用于集中服务器响应收到的 PADR 报文，并为此 PPP 会话分配资源。

⑤ PADT 用于终止 PPPoE 会话。

可通过 debugging pppoe-client all *interface-type interface-number* 命令查看报文交互过程。

命令：*debugging pppoe-client all*

例如：查看 Ethernet 0/0 接口对应的 Discovery 阶段报文交互过程如下。

```
* Jan  2 06:19:04:267 2007 client PPPOEC/7/debugging: Ethernet0/0: PPPoE clientout discovery packet (PADI), Len = 30

* Jan  2 06:19:04:270 2007 client PPPOEC/7/debugging: Ethernet0/0: PPPoE clientin discovery packet (PADO), Len = 60

* Jan  2 06:19:04:270 2007 client PPPOEC/7/debugging: Ethernet0/0: PPPoE clientout discovery packet (PADR), Len = 52

* Jan  2 06:19:05:738 2007 client PPPOEC/7/debugging: Ethernet0/0: PPPoE clientin discovery packet (PADS), Len = 60, Session ID = 1

* Jan  2 06:19:05:838 2007 client PPPOEC/7/debugging: Ethernet0/0: Created Dialer1:0 for PPPoE session
```

如果报文有丢失或异常，请检查网络情况及 PPPoE client 与 PPPoE server 协商参数是否匹配。

(4) 查看 PPPoE 发现阶段交互流程

PPPoE 建立过程分为两个阶段：发现阶段(PPPoE Discovery Stage)和会话阶段(PPPoE Session Stage)。会话阶段包括：LCP 阶段，Authentication 阶段(可选)、NCP 阶段(IPCP)、PPP 业务阶段(IP)，排查方法可参考云图 PPP 模块部分。

PPPoE server 故障排查

纪合宝





1. 开始

PPPoE(Point-to-Point Protocol over Ethernet,在以太网上承载 PPP 协议)的提出,解决了 PPP 无法应用于以太网的问题,是对 PPP 的扩展。PPPoE 将 PPP 报文封装在以太网帧之内,在以太网上提供点对点的连接。PPPoE 可以通过一个远端接入设备为以太网上的主机提供互联网接入服务,并对接入的每个主机实现控制、计费功能。

PPPoE 定位故障的思路是:先查看配置是否正确,之后根据协商阶段查看 Discovery 发现阶段与 Session 会话阶段报文交互过程。

2. 流程图相关操作说明

(1) 检查 PPPoE server 配置

检查配置应关注,VT 接口下 PPP 认证方式与用户名密码是否匹配,在太网接口上启用 PPPoE 协议,绑定虚拟模板接口。

命令:*display current-configuration*

例如:在设备上通过 display current-configuration 查看配置是否正确。

```
[H3C]display current-configuration
#
local-user 123                        //ppp 验证用户名与密码,与 PPPPOE client 使用用户名一致
 password cipher $c$3$pmkK8f9T7KmsLGvkXwVJs0d0WvsN4Q==
 service-type ppp
#
interface Ethernet0/0
 port link-mode route
 pppoe-server bind Virtual-Template 1   //在以太网接口上启用 PPPoE 协议,将该以太网接口与指定
                                        //的虚拟模板接口绑定
#
interface Virtual-Template1
 ppp authentication-modepap             //认证方式为 PAP
 remote address 1.1.1.2                 //给 client 分配地址 1.1.1.2
 ip address 1.1.1.1 255.0.0.0           //网关地址
#
```

(2) 查看 PPPoE 发现阶段交互流程

PPPoE 建立过程分为两个阶段:发现阶段(PPPoE Discovery Stage)和会话阶段(PPPoE Session Stage)。发现阶段获得对端的以太网 MAC 地址并确定一个 PPPoE SESSION_ID。

① PADI 用于 PPPoE client 发现 PPPoE 集中服务器,在 VLAN 内广播。

② PADO 用于集中服务器响应收到的 PADI 报文,声明自己能为 PPPoE client 提供服务。

③ PADR 用于 pppoe client 向特定的 PPPoE 集中服务器申请 PPPoE 服务。

④ PADS 用于集中服务器响应收到的 PADR 报文,并为此 PPP 会话分配资源。

⑤ PADT 用于终止 PPPoE 会话。

可通过 *debugging pppoe-server all interface-type interface-number* 命令查看报文交互过程。

命令：*debugging pppoe-server all interface-type interface-number*

例如：查看 Ethernet 0/0 接口对应的 Discovery 阶段报文交互过程如下。

```
* Jan  2 07:07:56:230 2007 server PPPOE/7/debug2:
  2007-1-2 7:7:56.228: PPPoE Event: Ethernet0/0,IN PADI packet

* Jan  2 07:07:56:230 2007 server PPPOE/7/debug2:
  2007-1-2 7:7:56.229: PPPoE Event: Ethernet0/0,OUT PADO packet

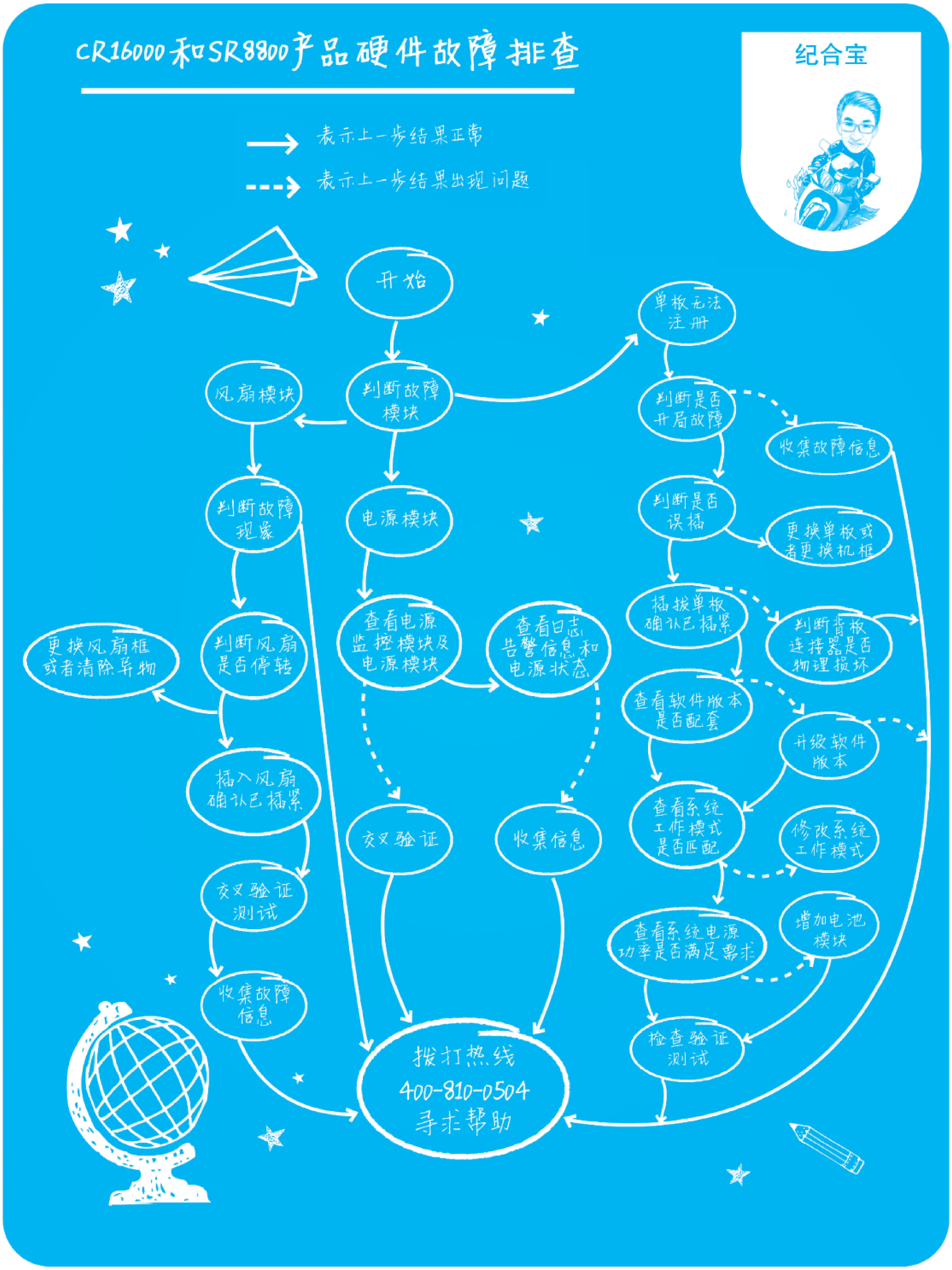
* Jan  2 07:07:56:239 2007 server PPPOE/7/debug2:
  2007-1-2 7:7:56.231: PPPoE Event: Ethernet0/0,IN PADR packet

* Jan  2 07:07:56:240 2007 server PPPOE/7/debug2:
  2007-1-2 7:7:56.237: PPPoE Event: Ethernet0/0, session 1 (Virtual-Template1:0), OUT
PADS packet
```

如果报文有丢失或异常，请检查网络情况及 PPPoE server 与 PPPoE client 协商参数是否匹配。

(3) 查看 PPPoE 发现阶段交互流程

PPPoE 建立过程分为两个阶段：发现阶段(PPPoE Discovery Stage)和会话阶段(PPPoE Session Stage)。会话阶段包括：LCP 阶段，Authentication 阶段(可选)、NCP 阶段(IPCP)、PPP 业务阶段(IP)，排查方法可参考云图 PPP 模块部分。


CR16000和SR8800产品硬件故障排查
纪合宝
表示上一步结果正常
表示上一步结果出现问题
开始
判断故障模块
风扇模块
判断故障现象
判断风扇是否停转
更换风扇框或者清除异物
插入风扇确认已插紧
交叉验证测试
收集故障信息
电源模块
查看电源监控模块及电源模块
查看日志告警信息和电源状态
交叉验证
收集信息
单板无法注册
判断是否子卡故障
收集故障信息
判断是否误插
更换单板或者更换机框
插拔单板确认已插紧
判断背板连接器是否物理损坏
查看软件版本是否配套
升级软件版本
查看系统工作模式是否匹配
修改系统工作模式
查看系统电源功率是否满足需求
增加电池模块
检查验证测试
拨打热线
400-810-0504
寻求帮助

1. CR16000/SR8800 产品硬件故障排查

CR16000/SR8800 产品出现硬件故障问题，首先应判断是哪一个模块出现了故障：风扇模块、电源模块或单板。

（1）CR16000/SR8800 产品出现风扇故障问题，首先应确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

如果风扇指示灯异常，或者命令行查询到风扇运行状态异常，或者设备打印风扇异常信息，则需要拔出风扇框观察确认是否有风扇停转，插拔风扇框并交叉验证确认故障，是否有异物。

确认故障后需要收集相关故障信息反馈 400。

如果风扇指示灯正常，命令行查询风扇运行状态正常，同时设备没有打印风扇异常信息，则说明风扇运行正常，如果还有疑问，请拨打 400-810-0504 寻求帮助。

（2）CR16000/SR8800 产品电源问题的主要排查思路是：先查看电源指示灯，根据电源指示灯排查确认是外部供电问题，还是电源模块自身的问题；如果电源指示灯正常，但是命令行显示电源状态异常，或者设备打印电源状态异常的日志信息，请直接收集故障信息反馈 400。

（3）CR16000/SR8800 产品出现单板无法注册问题，首先应判断是开局故障，还是运行中出现的故障。

如果是开局故障，则需要依次排查以下方面。

① 单板是否误插和单板是否插紧。

② 单板与设备运行的软件版本是否配套，如果是备用主控板，其版本是否和主用主控板一致。

③ 设备系统模式设置是否正确和系统电源功率是否满足要求。

④ 最后使用交叉验证的方式初步判定是否存在硬件故障。

如果是运行中出现故障，请直接收集故障信息并联系 400。

2. 流程图相关操作说明

（1）判断故障模块

从设备告警信息和指示灯判断是哪一个模块出现了故障：风扇模块、电源模块和单板。

（2）风扇模块

① 确认故障现象。确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

（a）风扇框指示灯说明。CR16000 风扇框指示灯说明如表 4-2 所示。

表 4-2　CR16000 风扇框指示灯说明

指示灯	颜　色	状　态	含　　义
RUN	绿色	灯灭	风扇框出现故障
		灯闪烁	风扇框处于正常运行状态
ALM	红色	灯灭	风扇框处于正常状态
		灯闪烁	风扇框处于故障状态
		灯常亮	

SR8800 风扇框指示灯说明如表 4-3 所示。

表 4-3 SR8800 风扇框指示灯说明

指示灯	颜 色	状 态	含 义
RUN	绿色	灯灭	风扇框出现故障
		灯常亮	风扇框处于正常运行状态
ALM	红色	灯灭	风扇框处于正常状态
		灯常亮	风扇框处于故障状态

(b) 命令行确认风扇运行状态,Normal 表示状态正常,Fault 和 Absent 表示状态异常,或者风扇框不在位。

```
CR16000
<H3C>display fan
Fan-tray state on chassis 0:
Fan-tray   1      state: Normal
SR8800
<H3C>display fan
 Fan     1 State: Normal
```

(c) 设备打印风扇异常信息如下。

```
%Jun 26 10:12:24:805 2013 H3C DEV/3/FAN_ABSENT:Fan 1 is absent.
%Jun 26 10:12:32:805 2013 H3C DEVD/2/DRV_DEV_FAN_CHANGE: Fan communication state
changed: Fan 1 changed to fault.
%Jun 26 10:12:42:405 2013 H3C DEV/2/FAN_FAILED:Fan 1 failed.
```

② 判断风扇是否停转,是否有异物。

(a) 拔出风扇框,(正常情况下,由于惯性的力量,风扇框在刚拔出来的时候,风扇的扇叶还是会继续旋转一段时间,如果有风扇没有在旋转状态,则说明该风扇之前已处于停止转动的异常状态)观察是否有风扇处于停止状态,如果有,则可以判断风扇故障,如果没有,请继续按照后续步骤排查。

(b) 拔出风扇框后,查看风扇框内是否有异物,如果有异物,会导致风扇运行异常,清除异物解决;如果确认没有异物,请继续按照后续步骤排查。

③ 插入风扇框确认插紧。风扇框没有插紧,会导致风扇运行状态异常。

(a) 插入风扇框,抬起风扇框插入机框风扇框槽位,向内缓慢推入到底;手动将风扇框面板两侧的松不脱螺钉导正后拧入,再使用螺丝刀拧紧螺钉,以确保良好固定。

(b) 观察风扇是否正常运行,指示灯状态是否正常,命令行查询风扇运行状态是否正常,是否有风扇异常信息打印;如果风扇运行恢复正常,则说明之前风扇框没有插紧;如果故障现象仍存在,请继续按照后续步骤排查。

④ 交叉验证。交叉验证,即把疑似故障的风扇框和正常运行的风扇框互换机框测试,确认故障是跟着风扇框走,还是跟着机框走;如果故障跟着风扇框走,则为风扇框故障,请更换解决,否则为机框故障,请按照后续步骤收集信息并将排查结果反馈 400。如果现场不存在交叉验证的条件,请按照后续步骤收集信息并反馈 400。

以上所有操作请在征得客户同意下进行,根据交叉验证的结果确认故障所在,拨打

400-810-0504 寻求帮助。

⑤ 收集故障信息。确认电源状态异常，或者日志中有电源异常告警信息，需要收集故障信息，反馈给 400 排查。

故障信息请收集设备的诊断信息、日志信息文件和 diagfile 文件。具体收集方法如下。

(a) 收集设备诊断信息。

命令：*display diagnostic-information*

执行完上述这条命令之后，请将在 CF 卡根目录中生成的 diag 文件导出来保存。

例如：

```
<H3C>display diagnostic-information
-----------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( * .diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

  0    drw-           -  Jul  07 2013 07:16:12   logfile
  1    drw-           -  Jul  07 2013 07:13:04   diagfile
  2    -rw-     4924407  May 06 2013 06:43:32   default.diag
  3    drw-           -  May 02 2013 03:31:52   diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

(b) 收集设备日志信息文件。

命令：*logfile save*

执行完上述命令后，将 CF 卡的 logfile 文件夹中的 logfile 文件全部导出来保存。

例如：

```
<H3C>logfile save
-----------------------------------------------------------------------
 Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

  0    -rw-  10484413  Dec 26 2013 08:37:00   logfile1.log
  1    -rw-    150941  Dec 14 2013 10:10:54   logfile.log
  2    -rw-    127193  Jan 21 2013 09:41:28   logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

(c) 收集设备 diagfile 信息文件。

(SR8800 的 R32XX 版本及之前版本，没有该文件，无须收集。)

在系统视图下输入_hide，进入到隐含模式，执行保存诊断文件的命令。

命令：*_diagnose-file save*

执行完上述命令后，将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如：

```
[H3C]_hide
Now you enter a hidden command view for developer's

testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's


direction.
[H3C-hidecmd]_diagnose-file save
------------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

    0   -rw-   2418760   Jul 09 2013 01:43:16    diagfile1.log
    1   -rw-     69266   Dec 03 2013 09:38:36     diagfile.log
    2   -rw-   4291181   Dec 10 2013 12:27:48    diagfile2.log
    3   -rw-    292979   Jul 07 2013 07:31:52    diagfile3.log
    4   -rw-   5240510   Jul 08 2013 11:55:00    diagfile4.log
    5   -rw-    110346   Jul 07 2013 08:51:44    diagfile5.log
    6   -rw-    192711   Jul 09 2013 12:03:26    diagfile6.log
    7   -rw-    166363   Jul 09 2013 08:38:20    diagfile7.log
    8   -rw-     17121   Jul 08 2013 16:37:48    diagfile8.log
    9   -rw-    101888   Jul 07 2013 07:54:28    diagfile9.log
   10   -rw-   2375568   Jul 09 2013 08:06:34   diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```

(3) 电源模块

① 查看电源监控模块和电源模块指示灯状态。电源监控模块和电源模块指示灯可直接反映电源的运行状态，排查电源问题请先查看电源监控模块（CR16000 特有）和电源模块指示灯状态，分别如表 4-4 和表 4-5 所示。

表 4-4 电源监控模块指示灯状态（CR16000 特有）

指示灯名称	颜色	状态	含 义
RUN	绿色	灯常亮	表示电源监控模块正常工作
		灯灭	表示电源监控模块有故障
MAJOR	红色	灯常亮	包括但不限于以下 4 种情况： ① 表示电源模块有故障 ② 电源框内所有电源模块被拔出 ③ 电源框开关关闭 ④ 电源模块在位，但未接入交流电
		灯先亮后灭	表示插拔电源模块
		灯灭	表示电源模块正常工作
MINOR	黄色	灯灭	保留

表 4-5 电源模块指示灯状态

指示灯名称	颜色	状态	含　　义
电源输入指示灯	绿色	灯常亮	表示电源输入正常
		灯灭	表示电源没有输入
		灯闪烁	表示电源输入超过最大范围
电源输出指示灯	绿色	灯常亮	表示电源模块输出正常
		灯灭	表示电源模块没有输出
		灯闪烁	表示电源模块输出过载
过温告警指示灯	黄色	灯常亮	表示电源模块过温告警
		灯灭	表示电源模块正常工作
电源故障指示灯	红色	灯常亮	表示电源模块出现故障
		灯灭	表示电源模块正常工作

② 依据指示灯状态做交叉验证。依据上一步骤中的指示灯状态列表，如果指示灯状态有异常，请根据指示灯状态，通过交叉验证确认故障所在，具体方法如下。

CR16000 的电源监控模块 RUN 灯灭、MAJOR 灯亮，表示电源模块有故障，请进一步查看电源模块指示灯状态。

(a) 如果电源模块输入指示灯灭，表示电源输入有问题，请交叉电源模块对应的电源线和供电线路，确认供电线路有无问题。如果现场不具备交叉验证的条件，请联系机房管理员进行检查确认。

(b) 如果电源模块输入指示灯正常，输出指示灯灭，表示电源输出有问题，请交叉电源模块，确认故障是否跟随电源模块走；跟随电源模块走，则为电源模块故障，否则为电源框故障；请将排查结果反馈 400。如果现场不存在交叉验证的条件，请按照后续步骤收集信息并反馈 400。

SR8800 直接查看电源模块指示灯状态。

(a) 如果电源模块输入指示灯灭，表示电源输入有问题，请交叉电源模块对应的电源线和供电线路，确认供电线路有无问题。如果现场不具备交叉验证的条件，请联系机房管理员进行检查确认。

(b) 如果电源模块输入指示灯正常，输出指示灯灭，表示电源输出有问题，请交叉电源模块，确认故障是否跟随电源模块走；跟随电源模块走，则为电源模块故障，否则为电源框故障；请将排查结果反馈 400。如果现场不存在交叉验证的条件，请按照后续步骤收集信息并反馈 400。

以上所有操作请在征得客户同意下进行，并确保设备供电充足，不会对客户业务造成影响。设备功耗计算请参考各产品的安装指导。根据交叉验证的结果确认故障所在，拨打 400-810-0504 寻求帮助。

③ 查看日志告警信息和电源状态。如果电源指示灯正常，通过命令行确认电源状态是否异常，设备是否打印电源状态异常的日志告警信息。

如果确认有电源状态异常或者日志中有电源异常告警信息，请按照下一步收集故障信息。如果电源状态正常，且日志中没有电源异常的告警信息，则说明电源是正常的。

查看日志信息命令：*display logbuffer*

查看电源状态命令：*display power-supply verbose*

例如：通过命令查看日志信息中的电源告警信息。

```
<H3C> display logbuffer
--------------------------------------------------------------------------
%@2551376%Mar 25 21:51:05:327 2013 H3C DEV/4/POWER FAILED:Chassis=1-Slot=0;
 Chassis 1 Power PSU 1/1/5 failed.
```

例如：通过命令查看电源状态。

```
<H3C> displaypower-supply verbose
--------------------------------------------------------------------------
PSU Status:
ID Status Input-Err Output-Err High-Temperature Fan-Err Closed Current-Limit
-- ------ --------- ---------- ---------------- ------- ------ -------------
1/1 Normal
1/2 Absent
1/3 Normal
1/4 Absent
1/5 failed
1/6 Absent
```

④ 收集故障信息。确认电源状态异常，或者日志中有电源异常告警信息，需要收集故障信息，反馈给 800 排查。

故障信息请收集设备的诊断信息、日志信息文件和 diagfile 文件，具体收集方法如下。

(a) 收集设备诊断信息。

命令：*display diagnostic-information*

执行完上述这条命令之后，请将在 CF 卡根目录中生成的 diag 文件导出来保存。

例如：

```
<H3C>display diagnostic-information
--------------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( *.diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

   0  drw-          -   Jul  07  2013  07:16:12  logfile
   1  drw-          -   Jul  07  2013  07:13:04  diagfile
   2  -rw-    4924407   May  06  2013  06:43:32  default.diag
   3  drw-          -   May  02  2013  03:31:52  diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

(b) 收集设备日志信息文件。

命令：*logfile save*

执行完上述命令后，将 CF 卡的 logfile 文件夹中的 logfile 文件全部导出来保存。

例如：

```
<H3C>logfile save
-----------------------------------------------------------------------
 Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

   0  -rw-  10484413  Dec  26  2013  08:37:00  logfile1.log
   1  -rw-    150941  Dec  14  2013  10:10:54  logfile.log
   2  -rw-    127193  Jan  21  2013  09:41:28  logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

(c) 收集设备 diagfile 信息文件。

(SR8800 的 R32XX 版本及之前版本，没有该文件，无须收集。)

在系统视图下输入_hide，进入隐含模式，执行保存诊断文件的命令。

命令：*_diagnose-file save*

执行完上述命令后，将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如：

```
[H3C]_hide
Now you enter a hidden command view for developer's

testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's


direction.
[H3C-hidecmd]_diagnose-file save
-----------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

     0  -rw-  2418760  Jul  09  2013  01:43:16  diagfile1.log
     1  -rw-    69266  Dec  03  2013  09:38:36  diagfile.log
     2  -rw-  4291181  Dec  10  2013  12:27:48  diagfile2.log
     3  -rw-   292979  Jul  07  2013  07:31:52  diagfile3.log
     4  -rw-  5240510  Jul  08  2013  11:55:00  diagfile4.log
     5  -rw-   110346  Jul  07  2013  08:51:44  diagfile5.log
     6  -rw-   192711  Jul  09  2013  12:03:26  diagfile6.log
     7  -rw-   166363  Jul  09  2013  08:38:20  diagfile7.log
     8  -rw-    17121  Jul  08  2013  16:37:48  diagfile8.log
     9  -rw-   101888  Jul  07  2013  07:54:28  diagfile9.log
    10  -rw-  2375568  Jul  09  2013  08:06:34  diagfile10.log
```

```
127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```

(4) 单板无法注册问题

① 判断是否是开局故障。设备开局时出现单板无法注册问题,可能的故障原因有很多,需要进一步排查;而设备运行中出现单板无法注册问题,可能的故障原因很少,硬件故障占了大多数。

所以如果是开局故障,请按照接下来的步骤继续排查;如果不是开局故障,而是设备运行中出现的故障,请直接收集故障信息并联系 400。

② 收集故障信息。故障信息请收集设备的诊断信息、日志信息文件和 diagfile 文件,具体收集方法如下。

(a) 收集设备诊断信息。

命令:*display diagnostic-information*

执行完上述这条命令之后,请将在 CF 卡根目录中生成的 diag 文件导出来保存。

例如:

```
<H3C>display diagnostic-information
------------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( * .diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

   0  drw-          -   Jul  07  2013  07:16:12  logfile
   1  drw-          -   Jul  07  2013  07:13:04  diagfile
   2  -rw-    4924407   May  06  2013  06:43:32  default.diag
   3  drw-          -   May  02  2013  03:31:52  diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

(b) 收集设备日志信息文件。

命令:*logfile save*

执行完上述命令后,将 CF 卡的 logfile 文件夹中的 logfile 文件全部导出来保存。

例如:

```
<H3C>logfile save
------------------------------------------------------------------------
 Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

   0  -rw-   10484413  Dec  26  2013  08:37:00  logfile1.log
   1  -rw-     150941  Dec  14  2013  10:10:54  logfile.log
   2  -rw-     127193  Jan  21  2013  09:41:28  logfile2.log
```

```
1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

(c) 收集设备 diagfile 信息文件。

(SR8800 的 R32XX 版本及之前版本，没有该文件，无须收集。)

在系统视图下输入_hide，进入到隐含模式，执行保存诊断文件的命令。

命令：*_diagnose-file save*

执行完上述命令后，将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如：

```
[H3C]_hide
Now you enter a hidden command view for developer's

testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's


direction.
[H3C-hidecmd]_diagnose-file save
------------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

    0  -rw-  2418760  Jul  09  2013  01:43:16  diagfile1.log
    1  -rw-    69266  Dec  03  2013  09:38:36  diagfile.log
    2  -rw-  4291181  Dec  10  2013  12:27:48  diagfile2.log
    3  -rw-   292979  Jul  07  2013  07:31:52  diagfile3.log
    4  -rw-  5240510  Jul  08  2013  11:55:00  diagfile4.log
    5  -rw-   110346  Jul  07  2013  08:51:44  diagfile5.log
    6  -rw-   192711  Jul  09  2013  12:03:26  diagfile6.log
    7  -rw-   166363  Jul  09  2013  08:38:20  diagfile7.log
    8  -rw-    17121  Jul  08  2013  16:37:48  diagfile8.log
    9  -rw-   101888  Jul  07  2013  07:54:28  diagfile9.log
   10  -rw-  2375568  Jul  09  2013  08:06:34  diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```

③ 判断是否误插。单板误插到非适配机型的机框上，会出现单板无法注册问题。

查看“H3C 技支通知 2014(007)号——关于下发《机箱式产品单板严禁混插说明(V1.0)》的通知”，或者查看单板的包装盒中附带的说明书，或者访问官网并搜索单板型号(单板型号可以在单板的前面板的右上角查看到)，确认单板是否和机框适配。

如果确认误插，请更换单板或者更换机框解决；如果不是误插，请按照后续步骤继续排查。

④ 插拔单板确认已插紧。单板没有插紧，或者单板后部的连接器故障，也会导致单板无法注册。

(a) 拔出单板后，首先判断单板后部与背板相连的连接器是否故障，是否受到物理损坏；如果是，请直接联系 400 更换单板解决；如果不是，请按照后续步骤重新插入单板，确保单板插紧。

(b) 插入单板时，要把单板前面板两侧的扳手往外翻，插入后要把将扳手向内合拢，使单板与背板紧密接触。

(c) 把单板前面板的螺钉拧紧，确保单板已固定。

⑤ 查看软件版本是否配套。新发货的单板与设备运行的软件版本不配套，会导致单板无法注册；如果是备用主控板，其发货版本和主用主控板不一致，也会出现无法注册的问题。

(a) 对于前一种情况，请查看设备运行版本的版本说明书，查看其中附录 A 的版本硬件特性列表里是否有该单板的型号列出。

如果能查到该单板型号，则说明软件版本和单板是配套的，请按照后续步骤继续排查。如果没有查到，可以确认软件版本与单板不配套，请访问官网并下载设备最新版本的版本说明书，按照上述相同的方法确认单板是否和最新版本配套，如果配套，则升级最新软件版本解决；如果单板和最新版本依然无法配套，请联系 400。

(b) 如果是备用主控板，需要检查其发货版本是否和主用主控板一致。检查方法如下。

把备用主控板插入机框，同时把 console 线接入到备用主控板上的 console 接口，查看备用主控板启动过程。在备用主控板的启动过程中，会显示备用主控板的启动版本，通过查看启动版本可以确认是否和主用主控板版本一致。

例如：查看 SR8800 备用主控板启动时打印的启动版本信息，启动版本是 R3342。

```
Press Ctrl+B to enter extended boot menu...
Starting to get the main application file--cfa0:/SR8800-CMW520-R3342.bin!
------------------------------------------------------------
```

如果确认备用主控板版本和主用主控板版本不一致，请查看备用主控板版本对应的版本说明书，参考其附录 B 中的“通过 BootWare 菜单升级启动文件”这一节，在 BootWare 菜单下同步备用主控板版本和主用主控板一致。如果确认备用主控板版本和主用主控板版本一致，请继续按照后续步骤排查。

⑥ 查看系统工作模式是否匹配。设备运行的系统工作模式和单板不匹配，会导致单板无法注册。

命令：*display system working mode*

(a) 通过上述命令可以查看设备运行的系统工作模式。

(b) 同时请查看单板所对应的产品的操作手册，在“01 基础配置指导-设备管理配置-配置系统工作模式”这一节中，可以查看到各类系统工作模式所支持的单板类型。

(c) 通过对比以上两步所查得的信息，可以确认单板是否和设备运行的系统工作模式匹配。

(d) 如果匹配，请继续排查后续步骤；如果不匹配，请调整系统工作模式解决。注意，调整系统工作模式需要重启设备才能生效。

例如：通过命令查看，可以确认 SR8800 的系统工作模式为 Hybrid。

```
<H3C>display system working mode
Current system working mode          :Hybrid
Working mode after system restart: Hybrid
Notice: Changing working mode will take effect only after system restart.
```

⑦ 查看系统电源功率是否满足要求。如果设备在增加单板后，设备总功耗大于系统电源输出功率，因为设备系统电源功率不足会导致单板无法注册问题。

这一步骤的排查方法是，先查询并计算出设备的总功耗和设备电源输出功率，再对比两者，如果设备总功耗小于设备电源输出功率，说明系统电源功率能够满足要求，请继续排查后续步骤；如果设备总功耗大于设备电源输出功率，说明系统电源功率不足，请增加设备电源模块解决。

查询和计算设备功耗和电源输出功率的方法：请查看对应产品安装指导的附录 A 章节，查找设备的单板、风扇的最大功耗值，和电源模块的最大输出功率值。把设备上所有的单板和风扇的最大功耗值相加，结果即为设备的整机功耗。确认设备上有几个电源模块，然后将电源模块数乘以电源模块的最大输出功率值，即为设备系统电源输出功率。

⑧ 交叉验证测试。经过前述步骤的排查，依然无法排除故障的话，请使用交叉验证排查是否存在硬件故障。

(a) 交叉验证测试的目的是为了初步确定是单板，还是主控板或者机框的硬件故障。

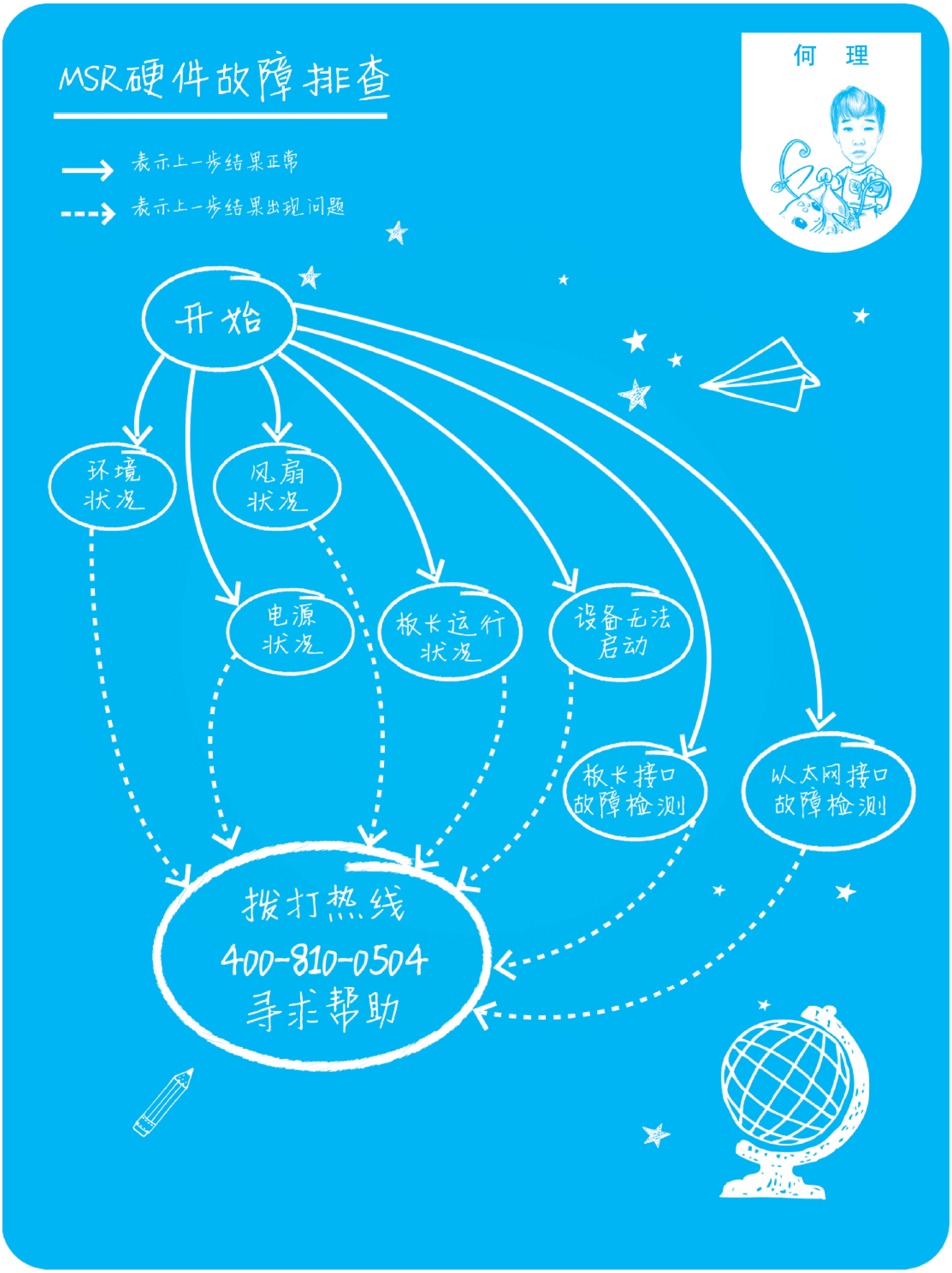
(b) 主要排查思路就是通过更换单板槽位的方式，确认故障是跟着单板转移，还是固定出现在某一槽位上。如果故障跟着单板转移，则可以初步确定是单板存在硬件故障；如果故障固定出现在某一槽位上，则可以初步确定是主控板或者机框存在硬件故障。

(c) 具体排查方法如下。

将无法注册成功的单板 A，和能够注册成功的单板 B 互换槽位测试。

如果单板 A 在新的槽位上依然无法注册成功，同时单板 B 能够注册成功，则可以初步确定是单板硬件故障导致无法注册成功；如果单板 A 在新的槽位上可以注册成功，同时单板 B 无法注册成功，则可以初步确定是主控板或者机框的硬件故障导致单板无法注册成功。

(d) 初步确定硬件故障位置后，请收集故障信息(收集方法已在前述步骤中有详细解释)，把交叉验证结果和故障信息反馈给 400。


MSR硬件故障排查
何 理
表示上一步结果正常
表示上一步结果出现问题
开始
环境状况
风扇状况
电源状况
板卡运行状况
设备无法启动
板卡接口故障检测
以太网接口故障检测
拨打热线
400-810-0504
寻求帮助

1. 开始

常见 MSR(V5)设备硬件故障可分为环境及单板硬件状态异常,板卡接口检测故障,以太网接口故障,其中常遇到的硬件问题为,单板无法注册,设备无法启动,接口无法 Up 等,硬件故障排查一般方法为：最常用的判断方法为替代测试,如果无法进行替代测试可根据对应设备调试命令,或设备异常堆栈信息进行判断。

2. 流程图相关操作说明

(1) 环境状态

各传感器温度应处于低温告警门限与一般级高温告警门限之间,如出现异常温度告警,比如：−1℃、255℃等,一般是软件版本问题或温度传感器硬件故障,需要更换硬件。

命令：*display environment*

例如：通过命令查看设备当前温度为 41℃,设置温度告警上限 60℃,下限 5℃。

```
<H3C> display environment
System Temperature information (degree centigrade):
-------------------------------------------------------
 SlotNo     Temperature     Lower limit     Upper limit
 0          41              5               60
```

(2) 风扇状况

风扇状态应该显示 Normal。如出现 Fault 或 Absent,建议重新插拔风扇尝试,如果运行时间较长,建议先除尘,并升级最新版本；如除尘,升级版本后问题仍然存在,建议更换风扇,对于集中式设备,建议更换设备。

命令：*display fan*

例如：通过命令显示设备风扇工作状态为 Normal。

```
<H3C> display fan

 Fan   1 State:Normal
```

(3) 电源状况

电源应该显示 Normal,如出现 Fault 或 Absent,建议重新插拔后尝试,并升级最新版本,如果设备只有一个电源,且该电源状态不正常,则更换电源或者设备；如果有多个电源,还需确认电源是否在位或者没有开电,如果确认电源在位、开电,电源状态异常,则更换电源或者设备。

命令：*display power*

例如：显示设备电源的状况为 Normal。

```
<H3C> display power

Power    0 State: Normal
```

(4) 板卡运行状况

所有业务板应该是 Normal,如果显示为 Fault 则表示该槽位单板出错,不能正常启动。

出现无法注册问题，或者不能识别问题，建议官网查看“接口模块手册-03-附录 B 适配关系章节”与版本手册，如果槽位适配关系与版本都符合要求，可进行替代测试，确认单板或主机故障，进行更换。

命令：*display device*

例如：设备板卡 SIC-1FEA 在槽位 1 上状态为 Normal。

```
<H3C> display device
 Slot No.   Board TypeStatus      Max Ports
 0      MSR20-21 RPU Board     Normal        12
 1      SIC-1FEA               Normal        1
```

(5) 设备无法启动

常见有下面 5 种情况。

① 找不到启动文件，请首先确认启动文件本身是否正常，可通过 md5 检验确认，之后判断是否为 Flash 故障导致启动文件异常，此时可以按 Ctrl+F 键格式化 Flash 后重新加载启动文件，如格式化过程报错，需要更换主机板。

② 电源无法上电，CON 口无反应，建议更换电源插座、电源线、PC、CON 线测试，如果确认都正常，可以进行主机更换。

③ 开机，按照提示进行内存检测，如果检测失败，进行主机更换。

④ 如果启动过程中出现“卡死”现象，建议拔掉所有单板后重启尝试，确认是主机故障还是板卡故障引起启动异常，进行相应设备硬件更换。

```
例如 1:
id=0x1cfff000, proc=0x18e11e0
Startup configuration file does not exist.
User interface con0 is available.
Press ENTER to get started.---敲回车，没有任何反应
例如 2:
system application si start id=Ox1a000fff, proc=0x20b29c4--打印此环节后无反应
```

⑤ 启动过程中，打印乱码或异常信息，可进行设备硬件更换。

```
例如:
id=0x1400300, proc=0x1a92368
id=0x2050000, proc=0x18500c8
id=0x2050fff, proc=0x1847178-----打印异常信息
Exception
Exception Number:             0x300
Exception Name:               DATA ACCESS EXCEPTION
Exception Instruction:        0x01AF1E40
Exception Slot:               0
Exception Task:               N/A (TID: -1)
Exception Stack Base:         0xffffffff
Exception Time:               2011-01-14   17:40:30
Exception Tick:               0x0(CPU Tick High) 0x4b59780d(CPU Tick Low)

Register contents:
Reg:  link[0], Val = 0x00000000 ; Reg:  link[1], Val = 0x00000000 ;
Reg:  link[2], Val = 0x00000000 ; Reg:  link[3], Va
```

（6）板卡接口故障检测

对于板卡接口类故障常见排查方法为接口替代测试，如果无法进行替代测试，可以进行接口打环测试，通过命令配置本地环回，查看接口是否检测到环回，是否 Up，如果打环测试失败，接口无法 Up，建议更换板卡；对于常用的 E1 与串口板卡，打环测试同时，还需要观察接口收发包是否一致(需先清空接口计数)，打环成功，收发包不一致，也需要硬件更换，具体判断方法可参考接口类型对应的云图章节。

（7）以太网接口故障检测

首先使用 *loopback internal* 命令对于以太网接口做环回测试，如果检测失败，直接进行模块或主机更换，如果成功，接口使用中无法 Up，可以用 PC 加交叉网线与该接口连接测试，在保证网线与 PC 正常情况下，接口依然无法 Up，可进行板卡或硬件更换更换。

```
固定三层接口：
[H3C-Ethernet0/0]loopback internal
%Jan  1 00:12:27:584 2007 client IFNET/3/LINK_UPDOWN: Ethernet0/0 link status is Up.
%Jan  1 00:12:27:585 2007 client IFNET/5/LINEPROTO_UPDOWN: Line protocol on the interface
Ethernet0/0 is Up.
[H3C-Ethernet0/0] display interface  Ethernet 0/0
Ethernet0/0 current state: Up
Line protocol current state: Up
Description: Ethernet0/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 5866-ba83-0f70
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 5866-ba83-0f70
Media type is twisted pair, loopback is set, promiscuous mode not set
二层交换接口：
 [H3C-Ethernet0/4]loopback internal
%Jan  1 00:13:05:645 2007 client IFNET/3/LINK_UPDOWN: Ethernet0/4 link status is Up.
[H3C-Ethernet0/4] display interface  Ethernet 0/4
 Ethernet0/4 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 5866-ba83-0f72
 Description: Ethernet0/4 Interface
 Loopback is set internal

H3C-Ethernet0/0]loopback internal
%Jan  1 00:12:27:584 2007 client IFNET/3/LINK_UPDOWN: Ethernet0/0 link status is Up.
%Jan  1 00:12:27:585 2007 client IFNET/5/LINEPROTO_UPDOWN: Line protocol on the interface
Ethernet0/0 is Up.
[H3C-Ethernet0/0] display interface  Ethernet 0/0
Ethernet0/0 current state: Up
Line protocol current state: Up
Description: Ethernet0/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 5866-ba83-0f70
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 5866-ba83-0f70
Media type is twisted pair, loopback is set, promiscuous mode not set
```


MPLS L2VPN(V7)故障排查
朱玉广
表示上一步结果正常
表示上一步结果出现问题
开始
公网路由是否正确
确认和修改ICP路由配置以及Loopback是否可达
MPLS LDP／LSP状态是否正常
确认和修改沿路MPSL及LDP配置
查看PW状态是否Up
确认和修改PW配置
拨打热线
400-810-0504
寻求帮助

1. MPLS L2VPN 故障排查

由与使用 LDP 方式的 MPLS L2VPN 通过 LDP 协议向远端通告本端 PW 标签等信息，报文转发是基于外层 LSP 的，而 LSP 是依附于路由的。所以定位故障的思路是：先查路由、再查 LSP/LDP，最后排查 MPLS L2VPN 配置。

2. 流程图相关操作说明

(1) 查看公网路由

确认是否在公网 LSP 途径的所有设备上都存在两端 PE 的 loopback 地址精确路由。

命令：*display ip routing-table*

例如：通过命令查看，可以确认存在对端 PE 的 Loopback 路由 2.2.2.2./32，下一跳是 10.0.0.2。

```
[H3C]display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask Proto Pre Cost    NextHop      Interface

2.2.2.2/32       O_INTRA 10   1    10.0.0.2     GE0/0
```

(2) 确认和修改公网 IGP 配置

是否通过公网 IGP 将 PE 的 loopback 地址的路由发布出去。

例如：公网 IGP 使用 OSPF，查看 OSPF 配置，可以确认已将 PE 的 loopback 地址 1.1.1.1 发布进公网 OSPF 内。

```
[H3C]display current-configuration configuration ospf
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.0.0.1 0.0.0.0
```

(3) 查看公网 LSP 信息及 LDP 状态

查看整个 LSP 上的所有设备是否已经为两个 PE 的 loopback 地址正确的分配了公网标签，以及 LDP Peer 是否正常。

命令：*display mpls lsp*

display mpls ldp peer

例如：通过命令查看，到达 2.2.2.2 的 LSP 已经建立，LSP 状态正常。

```
[H3C]display mpls lsp
FEC                 Proto    In/Out Label    Interface/Out NHLFE
1.1.1.1/32          LDP      3/-             -
2.2.2.2/32          LDP      1151/3          GE0/0
2.2.2.2/32          LDP      -/3             GE0/0
10.0.0.2            Local    -/-             GE0/0
```

```
[H3C]display mpls ldp peer
Total number of peers: 1
Peer LDP ID          State         Role     GR    MD5   KA Sent/Rcvd
2.2.2.2:0            Operational   Passive  Off   Off   34/33
```

(4) 确认和修改公网 MPLS 配置

在沿途所有设备上全局开启 MPLS 和 MPLS LDP,并在接口下配置 MPLS 和 MPLS LDP。

例如:本端 PE 上设置 mpls lsr-id1.1.1.1,全局和接口下开启 MPLS 和 MPLS LDP,命令为 *mpls enable* ,*mpls ldp enable*。

```
[H3C]display current-configuration
#
mpls lsr-id 1.1.1.1
#
mpls ldp
#
interface GigabitEthernet0/0
 mpls enable
 mpls ldp enable
```

(5) 查看 PW 状态

分别查看两端 PE 路由器的 PW 状态以及 AC 接口状态是否 Up。

命令:*display l2vpn xconnect-group verbose*

例如:通过命令查看,查看与 Peer 2.2.2.2 建立的 PW-ID 为 123 的 PW 状态正常。AC 接口状态正常。

```
[H3C]display l2vpn xconnect-group verbose
Xconnect-group Name :1
 Connection Name     : 1
  Connection ID      : 0
  State              : Up
  MTU                : 1500
  LDP PWs:
    Peer          PW ID          Link ID       State
    2.2.2.2       123            1             Up
  ACs:
    AC                           Link ID       State
    GE0/1                        0             Up
```

(6) 确认和修改 PW 配置

查看配置交叉连接组,绑定 AC 接口,并指定对端 loopback 地址,而且 pw-id 以及 pw-class 必须一致。

例如:创建交叉连接组 1,创建交叉连接 1,在交叉连接下绑定 AC 接口,并指定与对端(2.2.2.2)建立 PW,PW-ID 为 123,同时引用 PW 模板 1。

```
[H3C]display current-configuration configuration xcg
#
xconnect-group 1
```

```
connection 1
  ac interface GigabitEthernet0/1
  peer 2.2.2.2 pw-id 123 pw-class 1
#
[H3C]display l2vpn pw-class
Total number of PW classes: 1

PW Class Name        PW Type          Control Word   VCCV CC        VCCV BFD
1                    Ethernet         Enabled        Control-Word   BFD
```


配置策略路由后业务不通故障排查
表示上一步结果正常
表示上一步结果出现问题
何 理
开始
检查网络连通性
查看ACL策略是否正确
修改ACL策略
检查下一跳/出接口配置
下一跳/出接口是否生效
确保下一跳/出接口生效
拨打热线
400-810-0504
寻求帮助

04 路由器产品 > 4.2 SR66 产品 > 4.2.1 配置策略路由后业务不通故障排查 > 步骤详解

1. 开始

策略路由的作用是依据用户配置的策略进行报文转发，其关键在于所需执行的动作。所以定位故障的思路是：先排查 ACL 策略、再排查节点动作。

2. 流程图相关操作说明

(1) 检查网络连通性

首先检查网络连通性，确保在不配置策略路由时业务正常。

(2) 查看 ACL 策略是否正确

检查与策略路由相关 ACL 策略的配置与应用是否正确。

如果设备上存在多个策略路由或策略路由存在多个节点，需注意同一 ACL 被多次应用或者不同 ACL 中 RULE 相同的情况(可能导致相关报文转发出接口/下一跳错误)。

命令：***display policy-based-route*** [*policy-name*]

display acl { *acl-number* | *all* | *name acl-name* }

例如：配置 ACL 策略 3000，匹配源地址为 192.168.1.1 的 IP 报文以及源地址为 192.168.1.3 的 WWW 报文，并将其应用到策略路由 h3c 的 Node 20。

```
[H3C]display policy-based-route h3c
 Policy based routing configuration information:
 policy-based-route : h3c
    Node 20 permit :
        if-match acl 3000
      apply ip-address next-hop 11.0.0.1

[H3C]display acl 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's

step is 5
 rule 0 permit ip source 192.168.1.1 0
 rule 5 permit tcp source 192.168.1.3 0 source-port eq www
```

(3) 修改 ACL 策略

ACL 策略配置与应用不正确可分以下三种情况。

① ACL 策略本身配置错误，没有正确引流——请修改 ACL 策略配置。

② ACL 策略配置正确，但是被应用到其他策略路由或者此策略路由的其他节点——请将 ACL 策略正确调用到相应的策略节点。

③ ACL 策略配置不精确，导致不该匹配该策略路由的业务报文，经此策略路由转发，导致这些业务转发不通——请修改 ACL 规则，仅匹配所需业务报文即可。

(4) 检查下一跳/出接口配置

策略路由中，每个节点可以配置多个 apply 动作。在下一跳(next-hop)动作与出接口(output-interface)动作同时配置的情况下，下一跳动作优先执行，所以先检查下一跳动作配置，然后再检查出接口动作配置。

如果配置了下一跳动作，请检查配置的下一跳地址是否正确。例如，以下配置将下一跳地

址配置为10.0.0.2。

```
[H3C]display policy-based-route h3c
 Policy based routing configuration information:
 policy-based-route : h3c
    Node 10 permit :
       if-match acl 3000
       apply ip-address next-hop 10.0.0.2
```

如果配置了出接口动作，请检查配置的出接口是否正确。建议指定的出接口为P2P类型接口，当配置出接口为非P2P接口时(例如以太网接口)，可能会造成转发不通。例如，以下配置指定出接口为Serial0/0。

```
[H3C]display policy-based-route h3c
 Policy based routing configuration information:
 policy-based-route : h3c
    Node 10 permit :
       if-match acl 3001
       apply output-interface Serial0/0
```

(5) 下一跳/出接口是否生效

策略路由动作：指定下一跳。

需确保配置的下一跳地址可达。例如：通过ping测试，确认了下一跳10.1.1.1可达。

```
[SR66]ping 10.1.1.1
  PING 10.1.1.1: 56 data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

策略路由动作：指定出接口。

需确保出接口物理/协议Up。

如果知道下一跳地址，也建议使用ping测试保证下一跳地址可达。

例如：示例中Serial 1/0为Down状态，而且没有配置IP地址，需确保接口Up以及IP地址配置正确。

```
[SR66]dis ip int b
 * down: administratively down
 (s): spoofing
Interface                Physical  Protocol  IP Address     Description
Serial1/0                down      down      unassigned     Serial1/0...
```

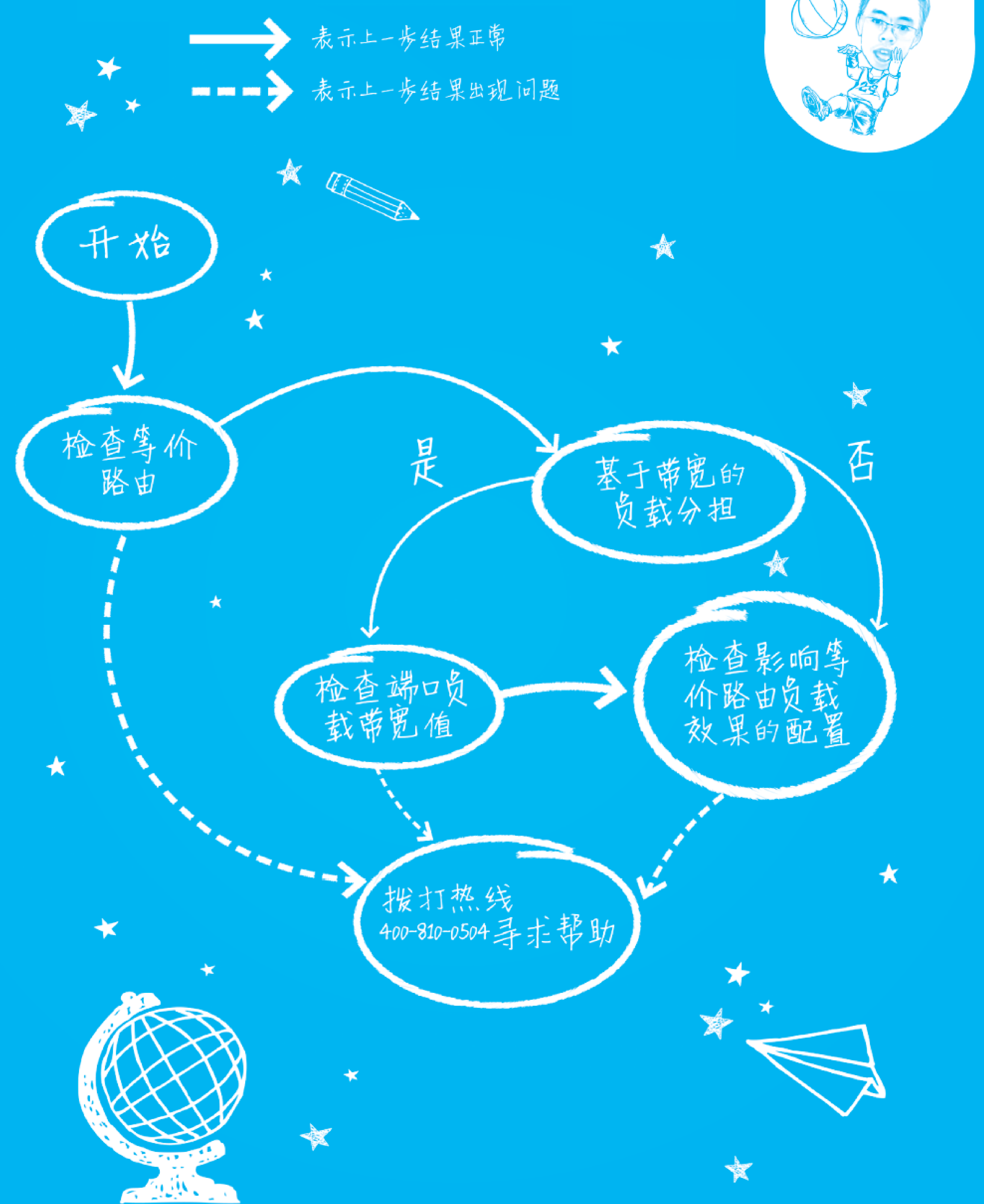
如果下一跳/出接口均生效，请拨打热线电话400-810-0504寻求帮助。

(6) 确保下一跳/出接口生效

检查相关接口、链路以及对端设备，保证下一跳/出接口生效。

等价路由不能达到负载效果故障排查

马文斌



1. 开始

定位故障的思路是：先查看是否形成等价路由，再确定需求是否为基于带宽的负载分担。基于带宽时，要确定相关端口的负载带宽配置；不基于带宽时，要确认是否存在影响等价路由负载效果的配置。

2. 流程图相关操作说明

(1) 检查等价路由

查看设备的路由表，判断是否形成等价路由，如果未形成等价路由请拨打热线 400-810-0504 寻求帮助。

命令：***display ip routing-table*** *x.x.x.x*

例如：以下命令表示，去往目的地址 2.2.2.2 存在 2 条等价路由。

```
<H3C>display ip routing-table 2.2.2.2
Routing Tables: Public
        Destinations : 7        Routes : 8
Destination/Mask    Proto   Pre  Cost       NextHop     Interface
...
2.2.2.2/32          Static  60   0          10.1.1.2    GE0/0/0
                    Static  60   0          20.1.1.2    GE0/0/1
```

(2) 基于带宽的负载分担

如果需求是基于带宽的负载分担，请查看设备是否开启基于带宽的负载分担功能。

命令：*bandwidth-based-sharing*

例如：通过 *display this* 命令查看，确认设备已经开启基于带宽的负载分担功能。

```
<H3C>display this
...
#
bandwidth-based-sharing
#
```

如果需求不是基于带宽的负载分担，请跳过此步，进入步骤(4)。

(3) 检查端口负载带宽值

默认情况下，接口负载带宽为接口的物理带宽。

可以通过命令，修改接口负载带宽值，实现基于一定比例的负载分担。

命令：***load-bandwidth*** *bandwidth*

例如：通过命令查看，确认接口的负载带宽为 1000。

```
[H3C-GigabitEthernet0/0/0]display this
#
interface GigabitEthernet0/0/0
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 load-bandwidth 1000
#
```

说明：如果上述负载带宽值设置为0，就会关闭当前接口的路由功能，该接口将不会被选择，但不对物理接口的其他状态产生影响。

如果确认此步骤配置正确后，仍然无法达到期望效果，请进入步骤(4)。

(4) 检查影响等价路由负载效果的配置

查看设备是否存在影响等价路由负载效果的配置，如策略路由、等价路由负载分担方式等。

策略路由优先级高于IP路由表。所以配置策略路由后，可能会影响到等价路由的负载效果。例如：通过命令查看，发现设备上配置了策略路由，指定下一跳为10.1.1.2。

```
<H3C>display policy-based-route
 policy-based-route : h3c
    Node 10 permit :
       if-match acl 2000
       apply ip-address next-hop 10.1.1.2
```

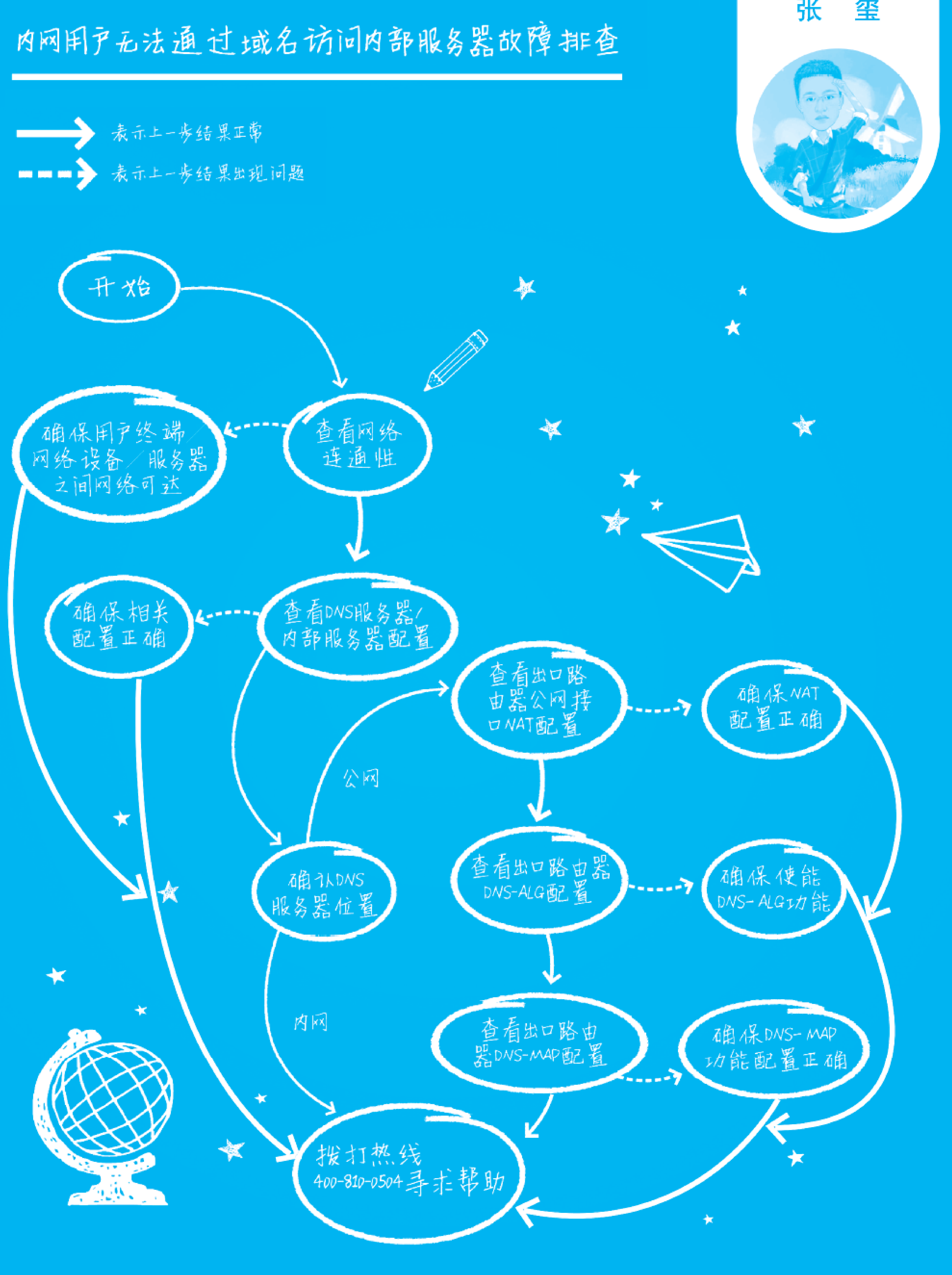
在基于流的负载分担方式中，可能会因为客户业务的原因，无法达到负载效果。可以通过配置基于报文的逐包负载分担方式解决此问题。

命令：***ip load-sharing mode*** { *per-flow* [*dest-ip* | *src-ip*] | *per-packet* }

例如：通过命令查看，设备的负载分担模式为基于报文目的IP地址的逐流负载分担。

```
<H3C>display this
ip load-sharing mode per-flow dest-ip
```

张 玺


内网用户无法通过域名访问内部服务器故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看网络连通性
确保用户终端/网络设备/服务器之间网络可达
查看DNS服务器/内部服务器配置
确保相关配置正确
确认DNS服务器位置
公网
内网
查看出口路由器公网接口NAT配置
确保NAT配置正确
查看出口路由器DNS-ALG配置
确保使能DNS-ALG功能
查看出口路由器DNS-MAP配置
确保DNS-MAP功能配置正确
拨打热线400-810-0504寻求帮助

1. 开始

当前，内网用户通过域名访问内部服务器在现网中已得到广泛应用。此类应用绝大多数与局域网出口路由器相关，本云图的排查思路也是基于此种情况。

排查时，请先查看网络连通性是否正常，再查看服务器配置是否正确，最后查看出口路由器的相关配置。

2. 流程图相关操作说明

(1) 查看网络连通性

需保证内网用户终端与 DNS 服务器、内网用户终端与内部服务器以及其他相关设备之间网络可达。

建议使用 ping 工具或者 Tracert 工具检查网络的连通性。

(2) 查看 DNS 服务器/内部服务器配置

DNS 服务器需处于正常工作状态，并配置相应域名和 IP 地址的映射。

例如：DNS 服务器上，配置了域名 www.abc.com 与 IP 地址 11.0.0.1 的映射，如图 4-1 所示。



图 4-1 www 属性

根据提供的业务，内部服务器需做相应的正确配置，此处不再赘述。建议内网用户可以尝试通过内部服务器的 IP 地址访问内部服务器，确保内部服务器的配置正确。

(3) 确认 DNS 服务器位置

如果 DNS 服务器位于公网，请跳过此步，进入步骤 4。

如果 DNS 服务器位于内网，则 DNS 服务器返回给内网用户的查询结果，其中的 IP 地址应为内部服务器的地址。此时，内网用户应可以通过域名访问内部服务器。

如果存在其他情况，请拨打热线 400-810-0504 寻求帮助。

(4) 查看出口路由器公网接口 NAT 配置

出口路由器公网接口需存在正确的 NAT 配置。

例如：以下命令通过 NAT Outbound 3000 将内网用户访问公网相关报文的源 IP 地址做了转换；通过 NAT Server 配置了公网 IP 地址与内部服务器 IP 地址的映射关系。

```
 #
acl number 3000
 rule 0 permit ip
```

```
#
interface GigabitEthernet5/0/1
 port link-mode route
 nat outbound 3000
 nat server protocol tcp global 11.0.0.1 www inside 192.168.1.2 www
 nat server protocol tcp global 11.0.0.1 8080 inside 192.168.1.3 8080
 ip address 11.0.0.1 255.255.255.0
#
```

(5) 查看出口路由器 DNS-ALG 配置

内网用户通过域名访问内部服务器时，出口路由器需要使能 DNS-ALG 功能。默认情况下，H3C 路由器 DNS-ALG 功能处于使能状态。

命令：*alg dns*

例如：通过查看出口路由器配置，发现 DNS-ALG 功能并未使能，使用命令使能 DNS-ALG 功能。

```
<H3C> displaycurrent-configuration
…
undo alg dns
…
<H3C>system
[H3C]alg dns
```

(6) 查看出口路由器 DNS-MAP 配置

如果内网中存在多台内部服务器为用户提供不同的业务(用户使用不同的域名，来访问不同的内部服务器)，但位于公网的 DNS 服务器中，这些不同的域名对应的是同一个公网地址，此时需要在出口路由器上配置 DNS-MAP 功能。

命令：*nat dns-map domain* ***domain-name*** *protocol* ***pro-type*** *ip* ***global-ip*** *port* ***global-port***

例如：内网存在两台内部服务器，内部用户使用域名 www.abc.com 访问内部服务器 192.168.1.2，使用域名 http://www.cba.com:8080 访问内部服务器 192.168.1.3。在公网 DNS 服务器上，域名 www.abc.com 以及 www.cba.com 对应的 IP 地址均为 11.0.0.1。

此时，可以在上述步骤(4)配置的基础上，添加 DNS-MAP 配置。

```
#
 nat dns-map domain www.abc.com protocol tcp ip 11.0.0.1 port www
 nat dns-map domain www.cba.com protocol tcp ip 11.0.0.1 port 8080
#
```


SR66系列路由器电源模块故障排查
表示上一步结果正常
表示上一步结果出现问题
何 理
开始
通过命令行查看电源状态
检查电源指示灯状态
检查电源供电及安装情况
交叉验证
拨打热线 400-810-0504寻求帮助
收集信息

1. 开始

SR66 系列路由器除了 SR6602 之外，可以配置两块或两块以上电源模块，从而达到冗余备份，路由器电源故障会对客户的网络造成极大的影响，即使是单电源故障也会给客户网络留下极大的隐患，所以一旦出现电源故障，需要在第一时间判断是否为电源模块问题。

排查思路：首先查看电源状态，然后查看电源指示灯状态，检查供电及电源模块安装情况，最后进行交叉验证。

2. 流程图相关操作说明

（1）通过 display power/display power-supply 命令查看电源状态

通过该命令查看电源状态是否为 Normal 状态，例如：

```
<Sysname> display power-supply
 Chassis 1 power-supply information
 ------------------------------------------------------------
  System Power Total                          : 1300 watts
  System Power Used(includes preassigned)     : 800 watts
  System Power Preassigned                    : 225 watts
  System Power Usable                         : 500 watts

  Power No.  Type   Watts   State    ID
  ---------------------------------------------
  1          AC     650     Normal   0
  2          AC     650     Normal   0
```

如果电源状态为 Normal 则表示电源供电正常，如果为 Failed 或者 Absent 状态则为不正常，请进行下一步操作。

SR66 系列路由器不同设备对 display power/display power-supply 命令的支持情况不一致，请参照命令手册。

（2）检查电源指示灯状态

电源指示灯可以直观地显示当前电源是否正常工作，SR66 系列路由器有两种电源模块，它们的电源指示灯略有差别。SR6602-X 路由器，可以通过观察面板的 PWR 指示灯，而 SR6604/08/16 以及-X 系列路由器则观察电源模块指示灯：如果电源指示灯不正常（常灭或者红灯常亮），则检查电源供电情况以及安装是否正确；如果电源指示灯正常（绿灯），但是设备依然显示为非 Normal，则进行交叉测试。

SR6602-X 电源指示灯状态如表 4-6 所示。

表 4-6　指示灯状态及说明

电　　源	状　　态	说　　明
PWR1	常灭	电源模块不在位
	绿灯常亮	电源模块供电正常
	红灯常亮	PWR2 供电正常是 PWR1 无电源输入或电源模块异常
PWR2	常灭	电源模块不在位
	绿灯常亮	电源模块供电正常
	红灯常亮	PWR1 供电正常是 PWR2 无电源输入或电源模块异常

SR6604/08/16 以及-X 系列路由器电源指示灯状态如表 4-7 所示。

表 4-7　指示灯状态及说明

电　　源	状　　态	说　　明
POWER	常灭	电源模块无输入
	绿灯常亮	电源工作正常
	红灯常亮	电源出现故障

(3) 检查供电以及安装是否正常

如果电源指示灯不亮或者电源亮红灯，请先检查一下电源线供电是否正常，并确保电源模块安装正确。

检查电源供电正常并且安装正确后，如果电源故障依然没有恢复则进行交叉替换测试。

(4) 电源模块交叉替换测试

最后需要进行电源模块的交叉替换测试，按照 A-B-A 方法测试，测试过程如下。

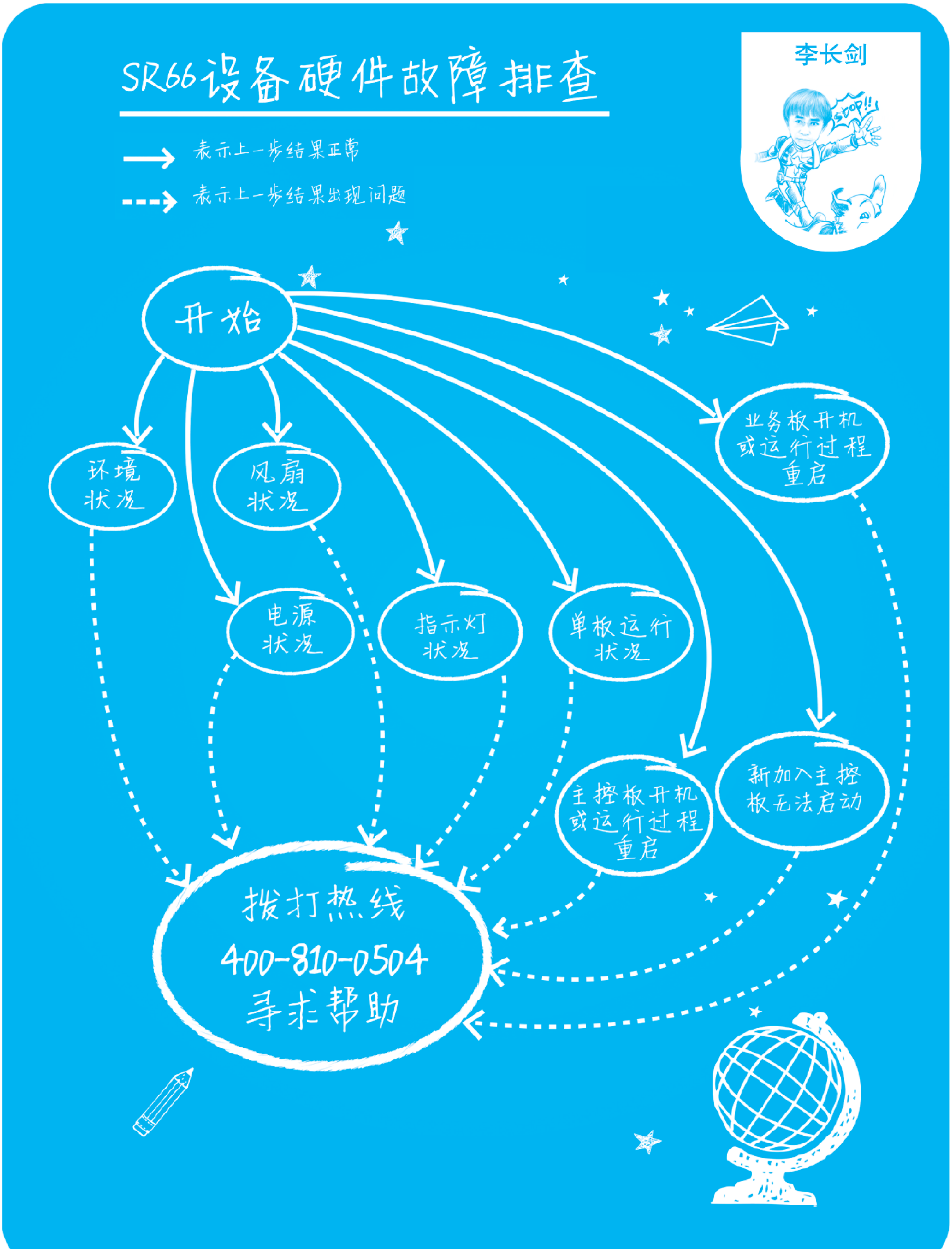
① 如果现场有两台设备，可以在保证单板正常供电的情况下直接进行替换测试，将故障电源与正常机框电源互换，观察是否正常启动，替换测试完成后再将故障电源插回原机框，观察是否正常启动(单板供电情况，可通过 display power-supply 命令查看或查看相关安装指导)。

② 如果现场只有一台设备，需要进行断电测试，将故障电源与正常工作电源互换，观察是否正常启动，然后再换回来，观察是否正常启动(单机替换测试，对客户业务会造成影响，请慎重操作)。

如果电源故障跟随电源模块走，则电源模块故障；如果替换测试后电源恢复恢复，则可能为其他问题；以上两种情况均需要收集步骤 4 相关信息，联系 400 热线处理。

(5) 收集信息

请反馈测试结果并收集以下信息，并联系 400 热线处理：①电源指示灯照片；②设备诊断信息；③故障时间的 Logfile 文件。


SR66设备硬件故障排查
李长剑
STOP!!
表示上一步结果正常
表示上一步结果出现问题
开始
环境状况
风扇状况
电源状况
指示灯状况
单板运行状况
业务板开机或运行过程重启
主控板开机或运行过程重启
新加入主控板无法启动
拨打热线
400-810-0504
寻求帮助

1. 开始

常见 SR66 设备硬件故障可分为环境及电源硬件状态异常，风扇故障，单板运行故障等，硬件故障排查一般方法为：最常用的判断方法为替代测试，如果无法进行替代测试可根据对应设备调试命令、诊断信息及 Logfile 信息进行判断。

2. 流程图相关操作说明

（1）环境状况

各传感器温度应处于低温告警门限与一般级高温告警门限之间，如出现异常温度告警，若是设备工作环境不佳，则可能出现温度超过正常工作范围的情况。

① 温度超过其上限时，会打印类似如下信息，此时风扇会全速转动以降低温度，建议采取措施改善设备工作环境的散热条件。

```
%Feb 29 16:22:25:31 2008 H3C DRVMSG/3/Temp2High:
 Environment temperature too high in Slot 2, index is 1.
```

② 超过临界温度时，会不断打印类似如下信息，建议立即下电出问题的单板，以免烧坏器件。

```
%Feb 29 16:33:24:377 2008 H3C DRVMSG/3/TempCritical:
 CPU temperature critical in Slot 4, index is 1.
```

③ SR6608 上出现类似如下信息时，建议立即断掉整个设备的电源，并观察有没有发生起火。

```
%Feb 29 16:06:24:377 2008 H3C DRVMSG/3/Temp2High:
 FAN temperature too high in Slot 9, index is 1.
```

命令：*display environment*

例如：通过命令查看设备当前温度为 slot0 24℃、slot1 26℃，设备温度告警上限 53℃，下限 0℃。

```
<H3C>display environment
 Temperature information (degree centigrade):
---------------------------------------------------------------
 SlotNo      Temperature        Lower limit       Upper limit
 0              24                  0                53
 1              26                  0                53
```

需要反馈：①设备诊断信息；②故障时间的 Logfile 文件；③如在现场，可感受风扇转速是否和设置转速匹配，并记录；④查看风扇灯的状态，并拍照。

（2）风扇状况

如果风扇发生故障，则会打印类似如下信息，SR6608 风扇框上红色 ALM 灯会常亮。

```
%Feb 29 13:53:04:857 2008 H3C DEV/4/FAN FAILED:
 Fan 1 failed.
```

出现故障现象时，按照如下顺序依次排查：①检查是否少安装了风扇；②检查是否有某个风扇停转；③SR6608 上检查风扇框是否插紧。

SR6608 在极端的情况下（风扇框温度超过 120℃），风扇也会停转，并提示类似如下的信息，此时请尽快断掉设备的电源。

```
%Feb 29 16:06:24:377 2008 H3C DRVMSG/3/Temp2High:
 FAN temperature too high in Slot 9, index is 1.
```

命令：*display fan*

例如：通过命令显示设备风扇工作状态为 Normal。

```
[H3C]dis fan
 Index   Status     Speedlevel
 ---------------------------
 1        Normal     2
```

需要反馈：① 设备诊断信息；② 故障时间的 Logfile 文件。

（3）电源状况

如果电源指示灯不亮，则可能电源接入电缆没有插紧/开关没开/电源故障；如果电源指示灯红色常亮，则可能电源模块没有插紧/电源故障/其他故障；如果电源指示灯绿色常亮，但控制台电源报警，则有可能电源故障/其他故障。

请进行相关排查或替换测试。

按照 A-B-A 方法测试，测试过程如下。

① 如果现场有两台设备，可以在保证单板正常供电的情况下直接进行替换测试，将故障电源与正常机框电源互换，观察是否正常启动，替换测试完成后再将故障电源插回原机框，观察是否正常启动。（单板供电情况，可通过 *display power-supply* 命令查看或查看相关安装指导）

② 如果现场只有一台设备，需要进行断电测试，将故障电源与正常工作电源互换，观察是否正常启动，然后再换回来，观察是否正常启动。（单机替换测试，对客户业务会造成影响，请慎重操作）

如果电源故障跟随电源模块走，则电源模块故障；如果替换测试后电源恢复，则可能为其他问题。

以上两种情况均需要收集相关信息：①电源指示灯照片；②设备诊断信息；③故障时间的 Logfile 文件。

命令：*display power*/*display power-supply*（SR66 系列路由器不同设备对命令的支持情况不一致，请参照命令手册。）

例如：显示设备电源的状况为 Normal。

```
<H3C> display power-supply

Chassis 1 power-supply information

---------------------------------------------------------

 System Power Total                          : 1300 watts
```

```
System Power Used(includes preassigned)        : 800 watts
 System Power Preassigned                      : 225 watts
 System Power Usable                           : 500 watts

 Power No.  Type    Watts    State    ID
 --------------------------------------------
 1          AC      650      Normal   0
 2          AC      650      Normal   0
```

(4) 指示灯状况

告警灯常灭，为正常现象，如告警灯常亮，表示设备发生严重问题，需要立刻查看系统日志和诊断信息。

业务板或主控板的 RUN 灯常灭，请查看单板运行情况。用命令查看单板电压是否正常。

命令：*[H3C-hidecmd]tshow voltage information slot #*

例如：查看设备 slot 3 槽位单板电压是否正常。

```
[H3C-old-hidecmd]tshow voltage information slot 3
  Slot  Index  Normal    Range      Current
   3     0      1.10    0.99-1.21    1.11
   3     1      1.20    1.08-1.32    1.24
   3     2      1.50    1.35-1.65    1.52
   3     3      1.80    1.71-1.89    1.81
   3     4      2.50    2.37-2.62    2.52
   3     5      3.30    3.13-3.46    3.32
   3     6      5.00    4.75-5.25    5.04
   3     7      0.00    0.00-0.00    0.00
```

需要反馈：①设备诊断信息；②故障时间的 Logfile 文件。

(5) 单板运行状况

所有业务板应该是 Normal，主控板为 Slave、master 状态，出现 Startup 一般为故障，需要插拔、替换测试；用命令查看单板电压是否正常；人员在现场时，首先查看单板灯的状态，并拍照；替换测试时，可以在线卡/主控的调试串口上插一个串口线，如果在启动的初始阶段出现内存检测错误的提示，可以进行内存插拔、除尘操作。

命令：*[H3C-old-hidecmd]tshow voltage information slot #*

例如：查看设备 slot 3 槽位单板电压是否正常。

```
[H3C-old-hidecmd]tshow voltage information slot 3
  Slot  Index  Normal    Range      Current
   3     0      1.10    0.99-1.21    1.11
   3     1      1.20    1.08-1.32    1.24
   3     2      1.50    1.35-1.65    1.52
   3     3      1.80    1.71-1.89    1.81
```

```
        3     4     2.50     2.37-2.62    2.52
        3     5     3.30     3.13-3.46    3.32
        3     6     5.00     4.75-5.25    5.04
        3     7     0.00     0.00-0.00    0.00
```

命令：*display device*

例如：设备板卡 FIP-20 在槽位 1 上状态为 Normal。

```
<H3C>display device
 System-mode(Current/After Reboot): Normal/Normal
 Slot No.   Board type          Status       Primary      SubSlots
 ---------------------------------------------------------------------
 0          SR6602-X1           Normal       Master         0
 1          FIP-20              Normal       N/A            2
```

需要反馈：①设备诊断信息；②故障时间的 Logfile 文件；③启动过程，包含内存提示信息。

(6) 主控板开机或运行过程重启

常见有下面 3 种情况。

① 找不到启动文件，确认启动文件本身是否正常或 CF 卡故障导致启动文件异常，此时可以按 Ctrl+F 键格式化 CF 卡后重新加载启动文件，如格式化过程报错，反馈启动过程、操作过程。

② 检查运行指示灯，如果运行指示灯不亮，有两种可能性：设备没有上电；Bootware 基本段被破坏。

③ 可能是内存或 CPU 本身有问题。对于 SR6602/02X，由于不能开机箱，反馈启动过程；对于其他设备，可以将内存拔掉测试。

需要收集：①设备启动过程、诊断信息；②故障时间的 Logfile 文件；③coredump。

(7) 新加入主控板无法启动

常见有下面 3 种情况。

① 同一设备两块主控板要求为同样型号，如不一致，需要更换解决。

② 同一设备两块主控板要求使用同样版本，新加入主控无法启动。

③ 内存：使用备用主控板自身的 Console 口连接 Console 线，查看启动状态、内存大小是否相同。

需要收集：①启动过程；②设备诊断信息；③故障时间的 Logfile 文件。

(8) 业务板开机或运行过程重启

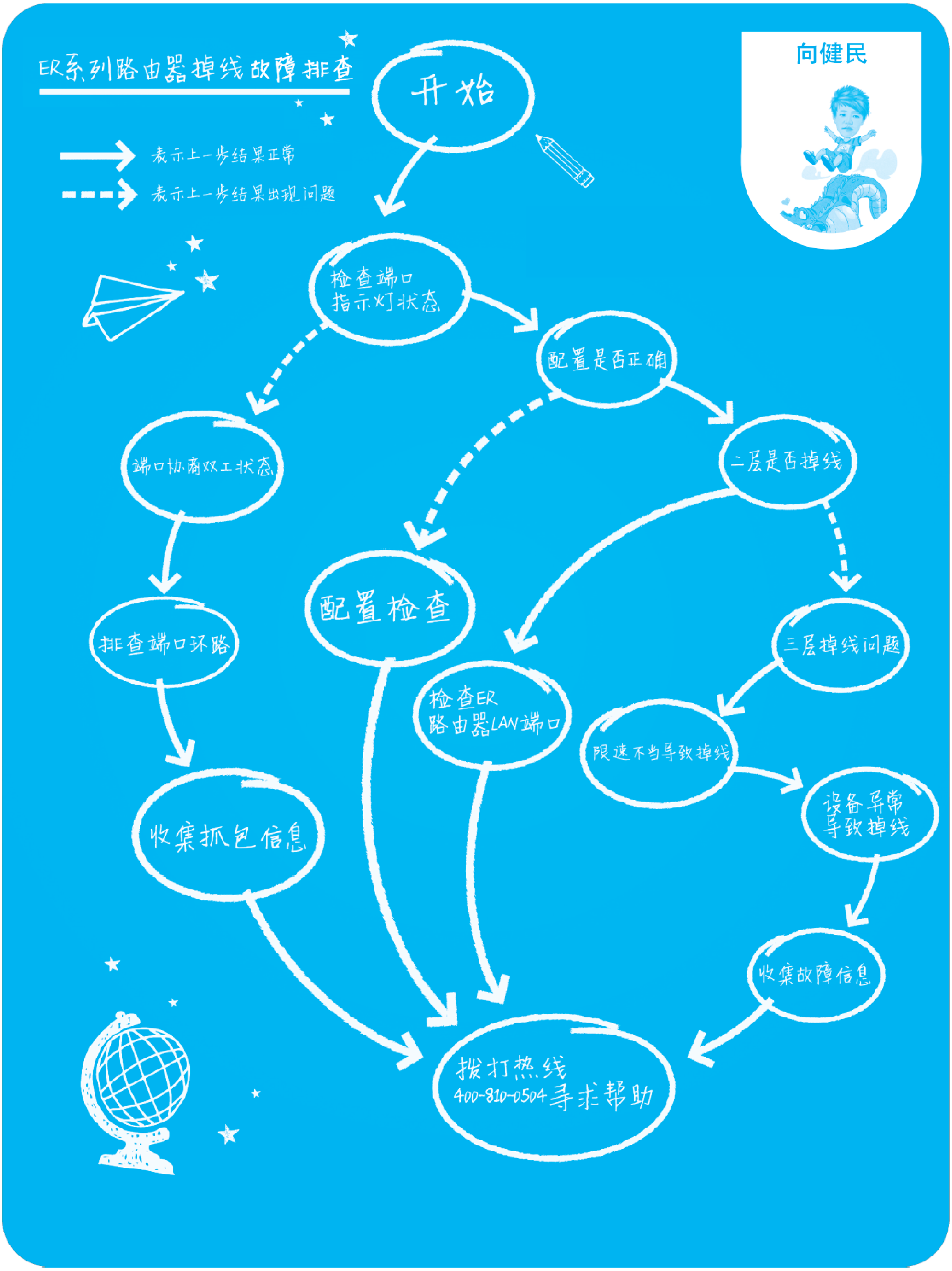
① 在板卡发生故障的时候，观察灵活接口平台上的电源指示灯是否灭掉，同时收集诊断信息；在诊断信息中，如果故障线卡的 reboot information 信息记录了多次非正常的 cold 冷启动记录，则是电源问题导致的故障。

② 使用同样方法确认设备上其他灵活接口平台是否有类似故障现象。如果其他板卡也有类似故障现象则说明是系统电源模块出问题，如果其他板卡都正常，说明是板卡自身问题。

③ 需要收集信息。

(a) 记录主控板、灵活接口平台 Console 口输出信息。

(b) 收集诊断信息和 CF 卡上的 Logfile 日志文件。



ER系列路由器掉线故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查端口指示灯状态
配置是否正确
端口协商双工状态
二层是否掉线
配置检查
排查端口环路
三层掉线问题
检查ER路由器LAN端口
限速不当导致掉线
设备异常导致掉线
收集抓包信息
收集故障信息
拨打热线
400-810-0504寻求帮助
向健民

1. 开始

ER 系列路由器采用全 Web 方式操作，定位于中小企业、网吧、经济酒店的宽带接入。根据客户网络的接入特点。所以定位故障的思路为：先检查硬件，其次检查配置，最后根据故障发生的网络层次进行定位（**硬件→配置→二层→三层**）。

2. 流程图相关操作说明

（1）检查端口指示灯状态

检查 ER 路由器端口指示灯，是否掉线时有：端口灯闪断（端口有短时间中断）、灯全亮、灯全灭、LAN 接口同时快闪烁的异常问题。

（2）端口协商双工状态

检查 ER 路由器端口指示灯状态，如表 4-8 所示，是否存在协商异常问题。

表 4-8　ER 路由器端口指示灯状态

指示灯	状态	含　义
Power	亮	供电正常
	灭	电源关闭或电源故障
W1/W2	亮	物理链路存在，并建立连接
	灭	物理链路存在，但未建立连接或物理链路不存在
100M	亮	端口工作在 100Mbps
	灭	端口工作在 10Mbps 或链路未建立
1000M	亮	端口工作在 1000Mbps
	灭	端口工作在 10/100Mbps 或链路未建立
Link/Act	亮	链路建立
	闪烁	端口在收发数据
	灭	链路未建立

登录 ER 路由器 Web 页面，检查 WAN 端口配置是否正常。具体操作为页面向导：接口设置→WAN 设置→网口模式。WAN 网口连接速度和双工模式如图 4-2 所示。

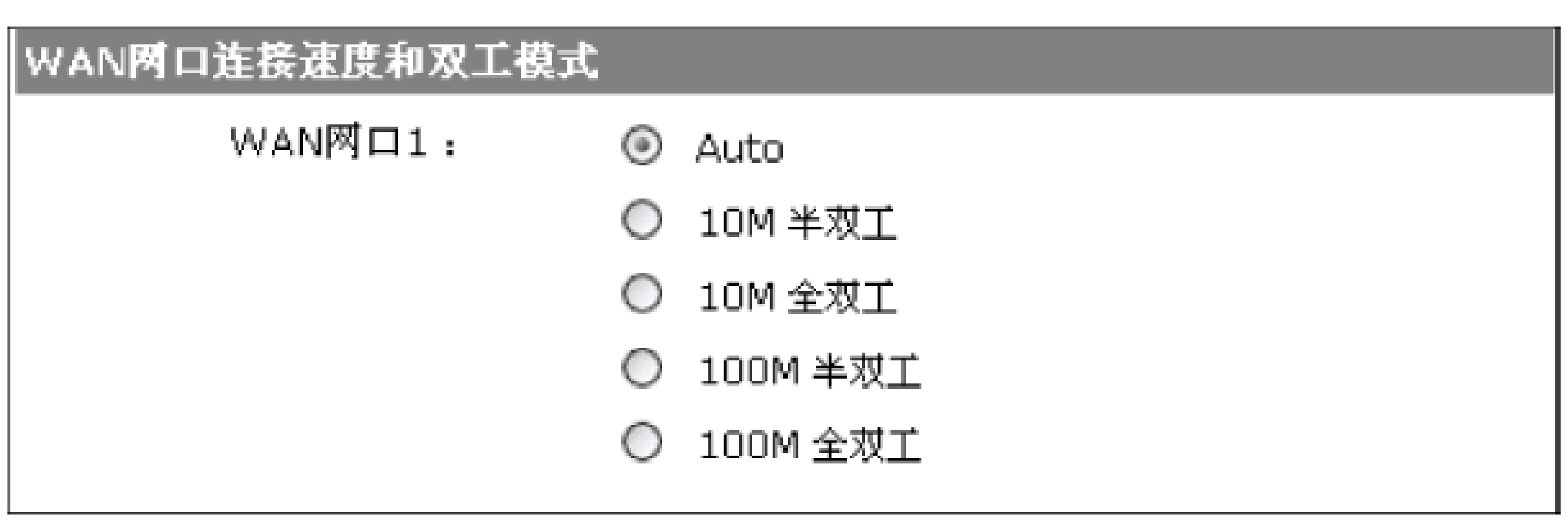


图 4-2　WAN 网口连接速度和双工模式

检查 LAN 端口配置是否正常。具体操作为页面向导：接口设置→LAN 设置→端口设置。端口设置如图 4-3 所示。

（3）排查端口环路

当 LAN 接口 Link/Act 灯出现同时快闪烁时，需排查是否因端口环路造成掉线。



图 4-3 端口设置

因 ER 路由器不支持 STP，建议先排查下联交换机是否存在环路。

ER 路由器可以通过设置"广播风暴抑制"为高，如图 4-4 所示，可暂时规避使得现象缓解，此时必须排查解决下联网络环路问题。具体操作为页面向导：接口设置→LAN 设置→端口设置。



图 4-4 设置"广播风暴抑制"为高

(4) 收集抓包信息

通过 ER 路由器的镜像功能，收集端口灯异常时的抓包信息，反馈给呼叫中心分析。具体操作为页面向导：端口管理→端口配置→端口镜像。端口镜像如图 4-5 所示。

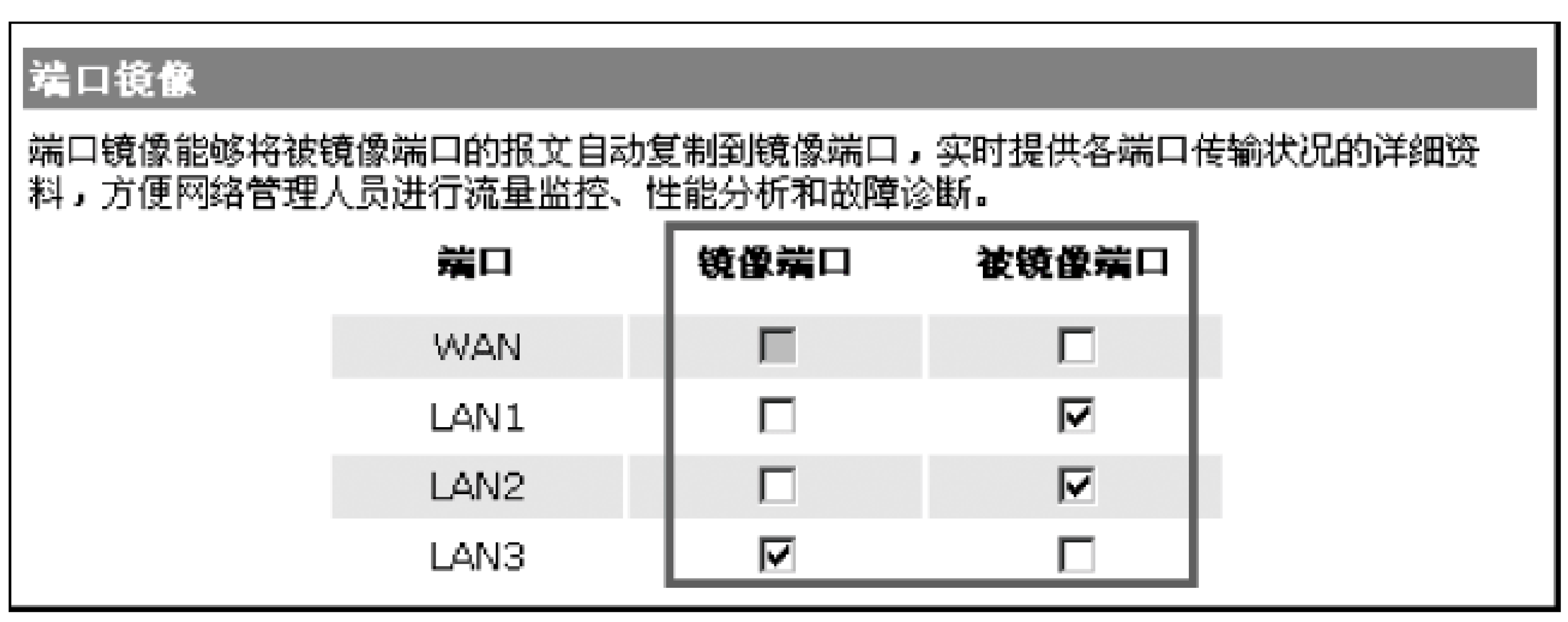


图 4-5 端口镜像

(5) 配置是否正确

检查 ER 路由器是否按照用户手册中"典型组网配置举例"章节配置设备。

《H3C ER 系列路由器用户手册》可在 H3C 中文网站中获取，具体操作为首页→服务支持→文档中心→路由器→H3C ER 系列路由器。

(6) 配置检查

检查 ER 路由器配置关键点是否按照要求配置，以下是为具体配置内容。

① 检查登录账号密码是否有弱口令风险，建议关闭 Web 和 Telnet 的远程访问。具体操作为页面向导：设备管理→用户管理→远程管理。

② 检查 ARP 防攻击是否配置，执行"安全专区→ARP 安全→ARP 防护"命令，选中"检测 ARP 攻击时，发送免费 ARP 报文"复选框，如图 4-6 所示。

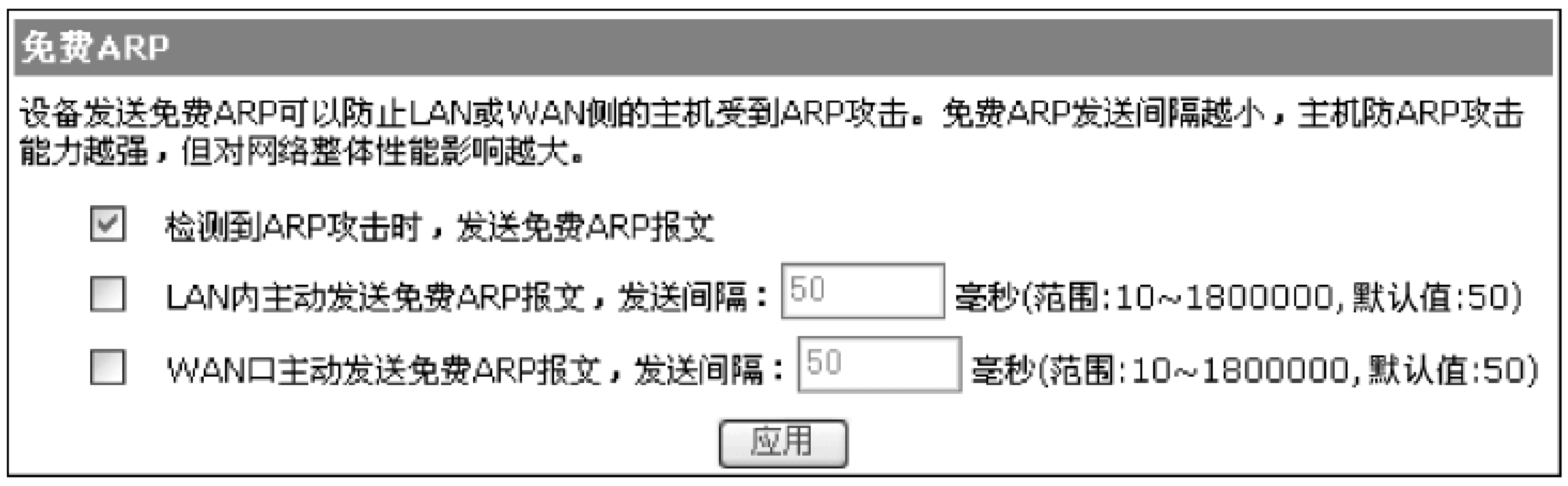


图 4-6 免费 ARP

③ 检查设置 QoS 设置。是否填写 WAN 真实带宽。起止 IP 是否包含全部上网 IP 地址。设置上下行限速是否合理。具体操作为页面向导：QoS 设置→流量管理→IP 流量限制。IP 流量限制如图 4-7 所示。

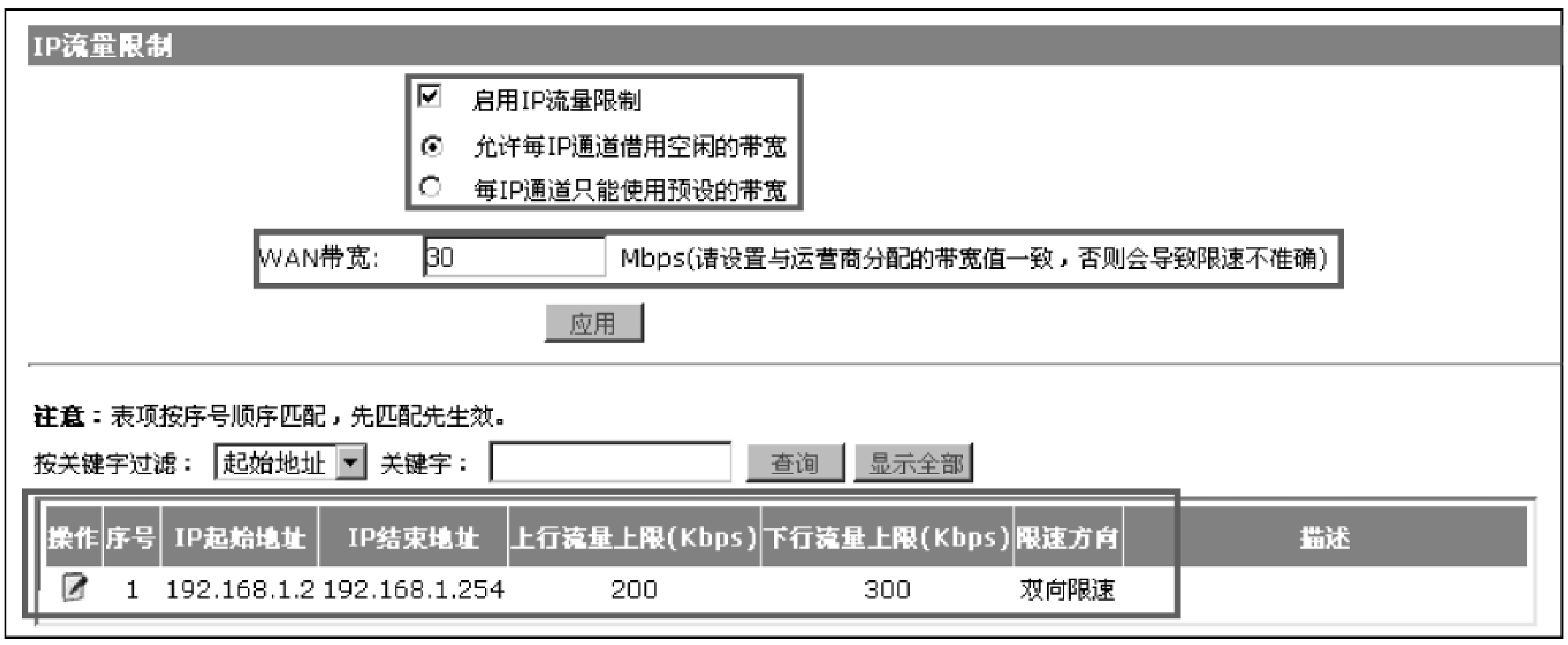


图 4-7 IP 流量限制

④ 检查 NAT 连接数限制。具体操作为页面向导：QoS 设置→流量管理→IP 流量限制→添加限速规则。网络连接限数——网页对话框如图 4-8 所示。



图 4-8 网络连接限数——网页对话框

如果配置内容较多，应用内容复杂，建议先备份 ER 路由器设备配置，恢复出厂设置后逐步增加配置项测试。**注意恢复出厂设置前，需备份用户设备配置**。具体操作为页面向导：设备管理→基本管理→配置管理。各过程截图如图 4-9 所示。

如果 ER 路由器 Web 页面内容与本指导有差异，建议升级 ER 路由器版本后进行配置。软件版本可从 H3C 中文网站获取，ER 路由器升级页面位置。具体操作为页面向导：设备管理→基本管理→软件升级。

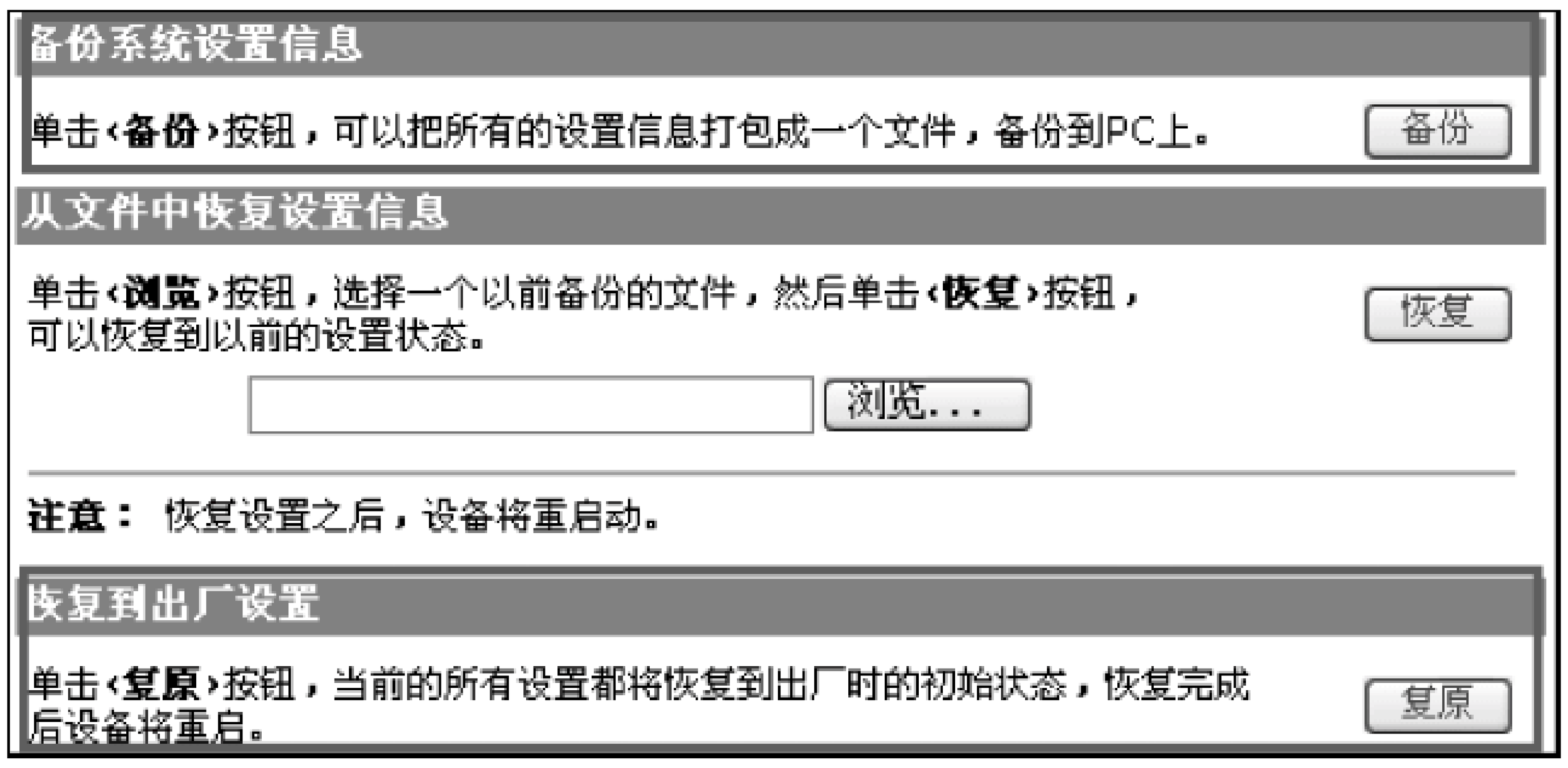


图 4-9　过程截图

说明：V10XRXX 系列软件版本，只能升级 V10X 系列设备硬件；V20X 系列软件，只能升级 V20X 系列设备硬件。

(7) 二层是否掉线

根据用户反馈现象，是否因为过二层原因造成的掉线，例如：①用户反馈掉线时，PC 之间互访也存在丢包或不通；②根据掉线用户的分布，为单个交换机下所有用户类掉线或 PC 互访存在问题；③复制内网文件时存在掉线问题。

如出现上述现象，建议按网络层，排查是否为二层转发问题。

(8) 检查 ER 路由器 LAN 端口

检查 ER 路由器 LAN 接口是否存在大流量互访流量。具体操作为页面向导：系统监控→流量监控→IP 流量。IP 流量情况如图 4-10 所示。

端口	发送流量(bit)	接收流量(bit)	发送速率(Kbps)	接收速率(Kbps)	链路状态
LAN1	2.97661G	28.6354M	356.796	36.313	100M全双工
LAN2	2.57633G	16.6253G	0	0	100M全双工
LAN3	16.6253G	2.57633G	0	0	100M全双工
WAN	11.0138M	42.4149M	1.206	4.272	100M全双工

清零　刷新

图 4-10　IP 流量情况

如图 4-10 所示，如果 LAN 接口之间，短时间存在大流量情况，需要检查流量是否超过端口速率导致的丢包。

检查 ER 路由器 LAN 接口设置，关闭流控开关，同时在下联的交换机口关闭流控开关，如图 4-11 所示。



图 4-11　关闭流控开关

将用户组网修改,只接一个 LAN 接口上行,排除二层流量经过 ER 造成的掉线问题。依据此步骤可排除 ER 路由器二层掉线问题,需对下联交换机等设备进行故障排查。

(9) 三层掉线问题

根据上一步故障现象判断,用户流量经过 ER 路由器后产生掉线问题。此类问题按用户可划分为部分用户掉线、全部用户掉线;根据时间分类为特定时间、随机时间掉线;根据特定条件划分为特定用户软件、特定流量触发掉线。上述问题一般需要收集 ER 路由器信息,提供呼叫中心热线做进一步分析和观察。

三层掉线问题后续步骤中给出部分可确认故障类型作为判断和解决方法。如无法解决,需联系呼叫中心收集故障信息。

(10) 限速不当导致掉线

ER 路由器支持 IP QoS 限速,需根据实际带宽和使用情况进行限速,限速不当可能导致单个用户或部分用户异常掉线。

① 例 1:如图 4-12 所示,单个用户掉线问题的排查。具体操作为页面向导:系统监控→流量监控→IP 流量。

在线主机数:29　在线主机的网络连接总数:1552

IP	总流量(bit)	速率(Kbps)	上行速率(Kbps)	限速前下行速率↑(Kbps)	限速后下行速率(Kbps)	网络连接数
192.168.1.40	12.2893G	1054.902	33.148	1055.146	1021.754	73
192.168.1.13	70.8626M	1070.426	57.133	1014.254	1013.293	186
192.168.1.5	29.4964G	1075.774	56.162	1013.1	1019.612	272
192.168.1.23	1.82341G	1053.252	25.784	992.593	1027.468	29
192.168.1.62	100.039G	1081.358	102.556	974.005	978.802	559
192.168.1.51	1.24569G	652.163	69.935	580.196	582.228	91
192.168.1.34	2.63621G	121.985	65.904	55.752	56.081	46
192.168.1.56	14.5500G	636.889	601.653	33.86	35.236	14
192.168.1.55	606.057M	25.716	7.698	17.88	18.018	4

第 1 页/共 4 页 共 29 条记录 每页 9 行 1 Go

图 4-12　IP 流量情况

如图 4-12 所示,用户下行限速为 1024Kbps,反馈异常用户 IP 为 192.168.1.62,从统计看流量已经占满导致掉线。此类问题需要用户关闭占用带宽的应用或在路由器上合理调整限速带宽。具体操作为页面向导:QoS 设置→流量管理→IP 流量限制,修改每 IP 上/下行流量上限。修改每 IP 上/下行流量上限如图 4-13 所示。

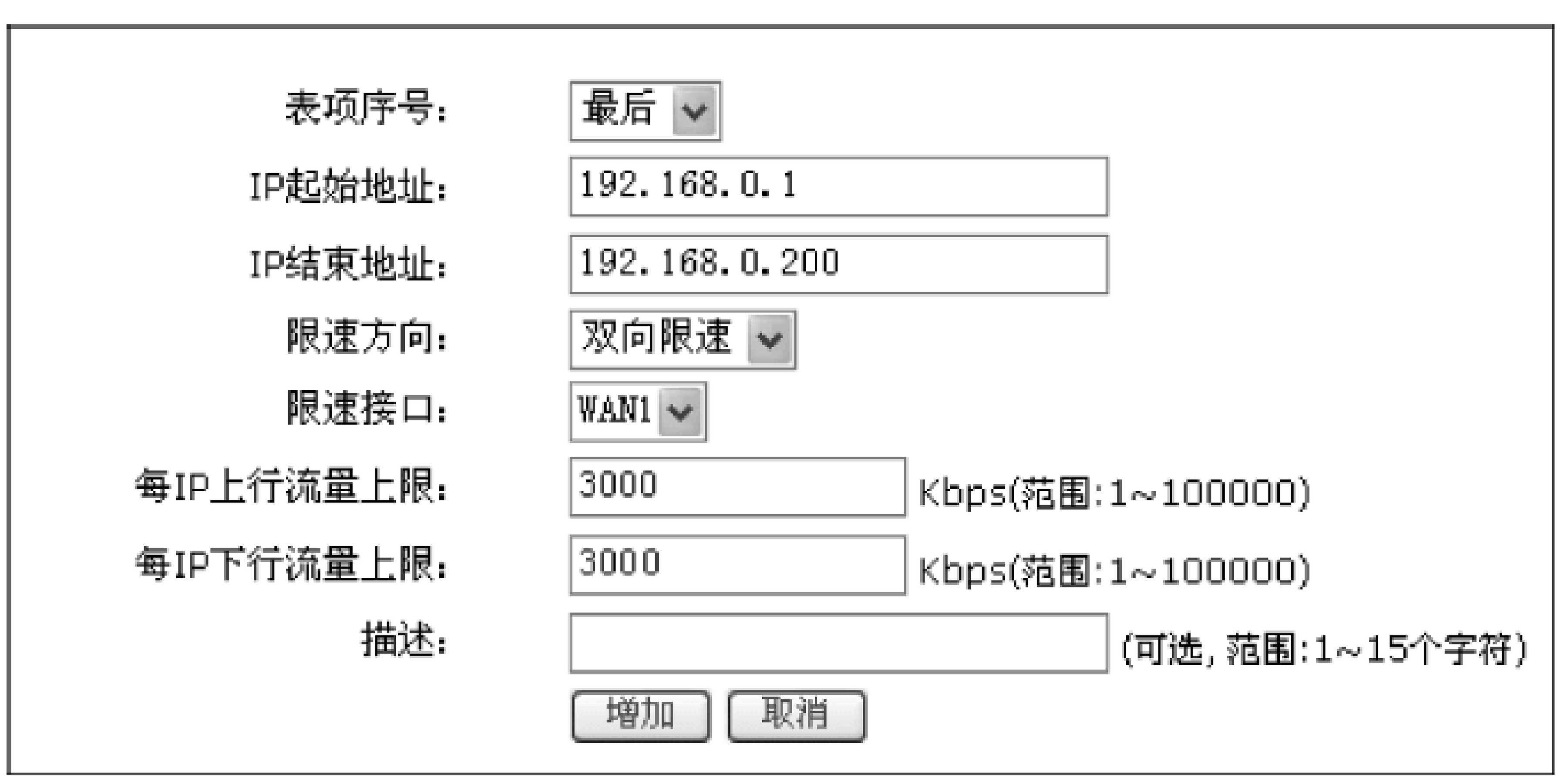


图 4-13　修改每 IP 上/下行流量上限

② 例 2：用户反馈部分用户存在掉线情况，需要查看，总带宽是否已经占满。具体操作是：“页面向导：系统监控→流量监控→端口流量。”端口流量情况如图 4-14 所示。

端口	发送流量(bit)	接收流量(bit)	发送速率(Kbps)	接收速率(Kbps)	链路状态
LAN1	220.295G	168.958G	4.473	3.016	100M全双工
LAN2	0	0	0	0	未连接
LAN3	348.559G	328.995G	2151.207	2065.412	100M全双工
WAN	486.832G	577.368G	1830.888	2039.192	100M全双工

图 4-14　端口流量情况

如图 4-14 所示，用户总带宽为 2Mbps，但用户 WAN 接收速率已经接近 2Mbps，导致用户掉线。此类问题可在路由器上调整 WAN 总带宽或向运营商申请更高带宽。具体操作为页面向导：QoS 设置→流量管理→IP 流量限制，调整 WAN 带宽。IP 流量限制如图 4-15 所示。

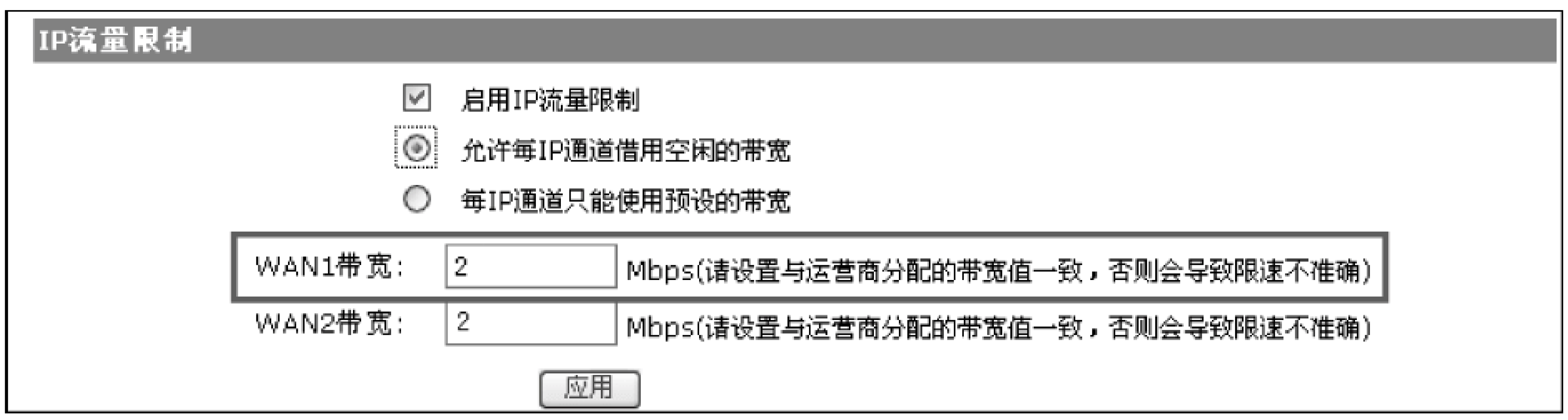


图 4-15　IP 流量限制

(11) 设备异常导致掉线

出现所有用户掉线时，需登录 ER 路由器，检查 ER 路由器日志，是否有异常日志。例如设备重启、WAN、LAN 接口 Up/Down 信息、CPU、内存占用高告警等日志。具体操作为页面向导：系统监控→系统日志→日志信息。日志信息如图 4-16 所示。

日志信息

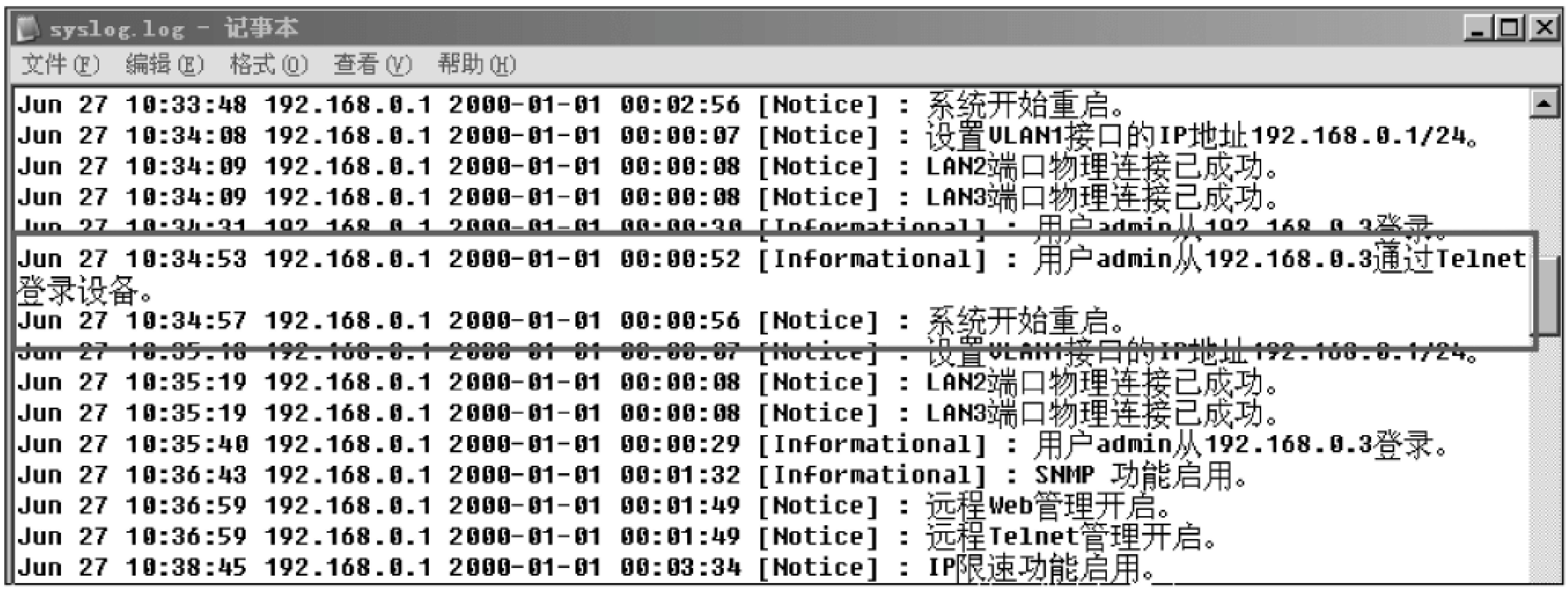
提示：点击日志信息的各属性标题，可进行排序；双击日志表项，可查看该日志详细信息和操作建议。

查询项：日期　关键字：请选择　查询　显示全部

	日期时间 ↑	级别	信息来源	信息内容
!	2013-06-09 10:15:06	Debug	流量信息	WAN接口接收流量已超过设定带宽值的90%。
!	2013-06-09 10:14:36	Notice	系统	WAN接口的DHCP客户端成功获取到IP地址10.165.16...
!	2013-06-09 10:14:33	Debug	系统	DHCP客户端从WAN口请求IP地址10.165.16.172。
!	2013-06-09 10:14:33	Debug	系统	DHCP客户端从WAN口发送DISCOVERY报文。
!	2013-06-09 10:14:29	Notice	系统	DHCP客户端从WAN口释放IP地址10.165.16.172。
!	2013-06-09 10:14:26	Debug	流量信息	WAN接口接收流量已超过设定带宽值的90%。

图 4-16　日志信息

① 如果有出现掉线时间和 ER 路由器重启时间大致一致，需搭建本地日志服务器，将日志发送到内网服务器上，在服务器上搭建 Syslog Server 接收日志，判断是否为非法用户登录设备造成重启，如有此情况可针对性的：修改 ER 路由器登录账号密码、关闭远程管理、关闭 SNMP 功能。如图 4-17 所示，Jun 27 10:34:53 用户 admin 登录后，Jun 27 10:34:57 系统开始重启，则可能为 admin 用户操作重启。



```
syslog.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Jun 27 10:33:48 192.168.0.1 2000-01-01 00:02:56 [Notice] : 系统开始重启。
Jun 27 10:34:08 192.168.0.1 2000-01-01 00:00:07 [Notice] : 设置VLAN1接口的IP地址192.168.0.1/24。
Jun 27 10:34:09 192.168.0.1 2000-01-01 00:00:08 [Notice] : LAN2端口物理连接已成功。
Jun 27 10:34:09 192.168.0.1 2000-01-01 00:00:08 [Notice] : LAN3端口物理连接已成功。
Jun 27 10:34:31 192.168.0.1 2000-01-01 00:00:30 [Informational] : 用户admin从192.168.0.3登录。
Jun 27 10:34:53 192.168.0.1 2000-01-01 00:00:52 [Informational] : 用户admin从192.168.0.3通过Telnet登录设备。
Jun 27 10:34:57 192.168.0.1 2000-01-01 00:00:56 [Notice] : 系统开始重启。
Jun 27 10:35:18 192.168.0.1 2000-01-01 00:00:07 [Notice] : 设置VLAN1接口的IP地址192.168.0.1/24。
Jun 27 10:35:19 192.168.0.1 2000-01-01 00:00:08 [Notice] : LAN2端口物理连接已成功。
Jun 27 10:35:19 192.168.0.1 2000-01-01 00:00:08 [Notice] : LAN3端口物理连接已成功。
Jun 27 10:35:40 192.168.0.1 2000-01-01 00:00:29 [Informational] : 用户admin从192.168.0.3登录。
Jun 27 10:36:43 192.168.0.1 2000-01-01 00:01:32 [Informational] : SNMP 功能启用。
Jun 27 10:36:59 192.168.0.1 2000-01-01 00:01:49 [Notice] : 远程Web管理开启。
Jun 27 10:36:59 192.168.0.1 2000-01-01 00:01:49 [Notice] : 远程Telnet管理开启。
Jun 27 10:38:45 192.168.0.1 2000-01-01 00:03:34 [Notice] : IP限速功能启用。
```

图 4-17 Syslog Server 接收日志

② 如果在掉线时,日志出现 WAN 或 LAN 物理接口 Up/Down 情况,可尝试更换网线。如图 4-18 所示,2013-06-09 10:19:15 WAN、LAN 物理接口出现断开情况,可相应地查看客户端掉线时间是否与其吻合。



日志信息

提示:点击日志信息的各属性标题,可进行排序;双击日志表项,可查看该日志详细信息和操作建议。

查询项: 日期 关键字: 请选择 查询 显示全部

日期时间	级别	信息来源	信息内容
2013-06-09 10:19:16	Notice	系统	DHCP客户端从WAN口释放IP地址10.165.16.172。
2013-06-09 10:19:15	Notice	系统	WAN接口物理连接已断开。
2013-06-09 10:19:10	Notice	系统	LAN2端口物理连接已断开。
2013-06-09 10:19:10	Notice	系统	LAN1端口物理连接已断开。

图 4-18 日志信息

③ 如果在掉线时出现 ER 路由器 CPU、内存占用高,可尝试设备防攻击设置,开启异常流量防护功能或在掉线时抓包联系呼叫中心进行分析。如图 4-19 所示 2013-06-09 10:19:07 CPU 使用率超过 90%,可相应地查看客户端掉线时间是否与其吻合,开启设备的防攻击设置,尝试是否解决。



日志信息

提示:点击日志信息的各属性标题,可进行排序;双击日志表项,可查看该日志详细信息和操作建议。

查询项: 日期 关键字: 请选择 查询 显示全部

日期时间	级别	信息来源	信息内容
2013-06-09 10:19:16	Notice	系统	DHCP客户端从WAN口释放IP地址10.165.16.172。
2013-06-09 10:19:15	Notice	系统	WAN接口物理连接已断开。
2013-06-09 10:19:10	Notice	系统	LAN2端口物理连接已断开。
2013-06-09 10:19:10	Notice	系统	LAN1端口物理连接已断开。
2013-06-09 10:19:07	Critical	系统	CPU使用率超过90%。
2013-06-09 10:19:01	Notice	系统	LAN2端口物理连接已成功。
2013-06-09 10:19:01	Notice	系统	LAN1端口物理连接已成功。
2013-06-09 10:18:53	Infor...	系统	用户admin从192.168.0.3通过Telnet登录设备。

图 4-19 日志信息显示异常

(12) 收集故障信息

当以上方法均无法解决时,需要收集 ER 路由器相关信息联系呼叫中心进行分析,相关操作如下。

故障发生时的设备信息收集，需登录 ER 路由器 Web 页面收集。具体操作为页面向导：系统监控→网络维护→一键导出。

搭建 Log 日志服务器，判断设备掉线异常时设备是否有相关日志上报。具体操作为页面向导：系统监控→系统日志→日志管理，设置日志等级为'debug(7)'，选中发送到日志服务器复选框，填写内网 IP 地址。过程截图如图 4-20 所示。

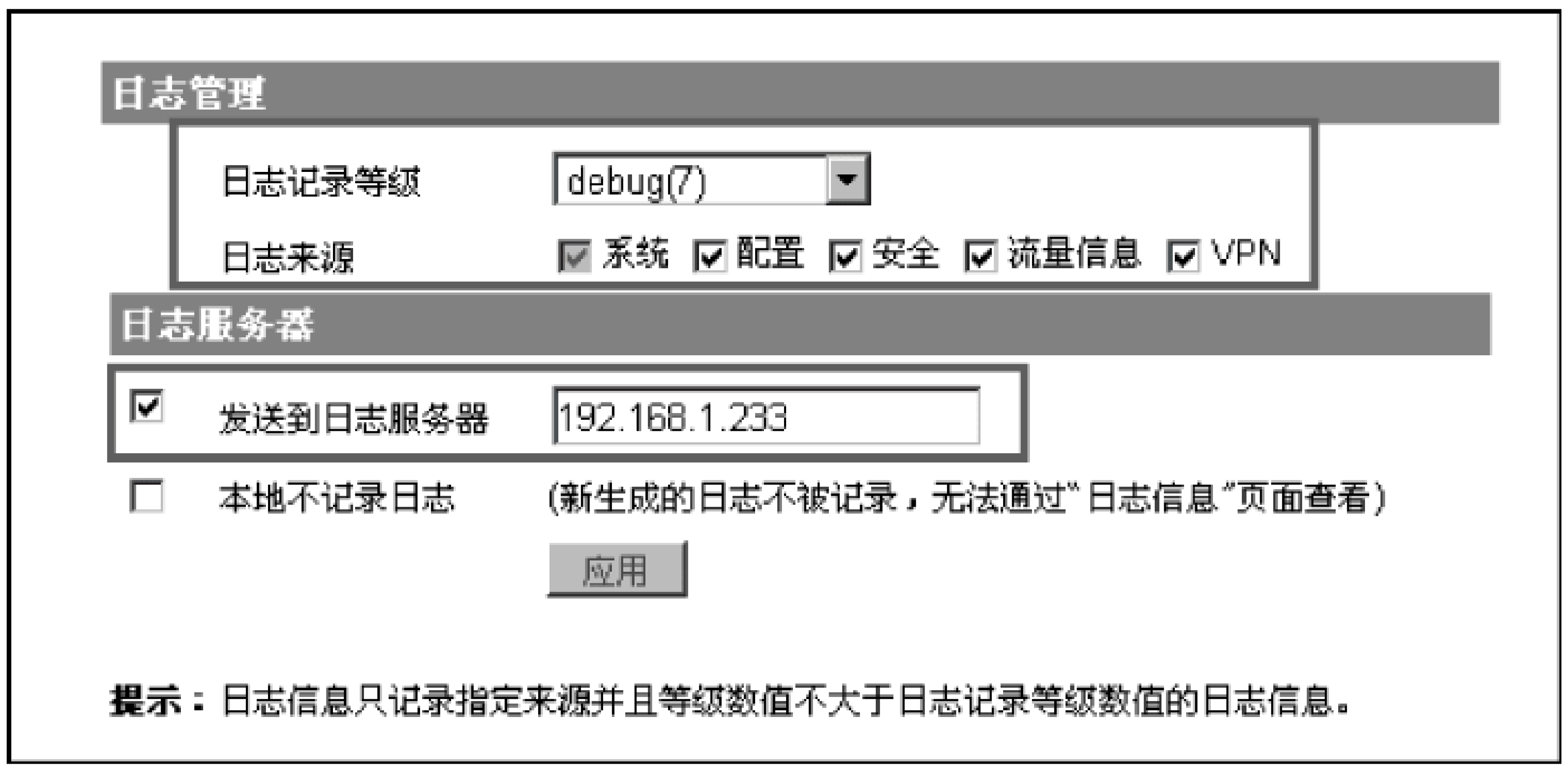


图 4-20　过程截图

搭建抓包环境，例如在 LAN3 口接一台抓包 PC，将 WAN 端口，LAN 业务端口镜像到 LAN3 口 PC 上。具体操作为页面向导：端口管理→端口配置→端口镜像。端口镜像如图 4-21 所示。

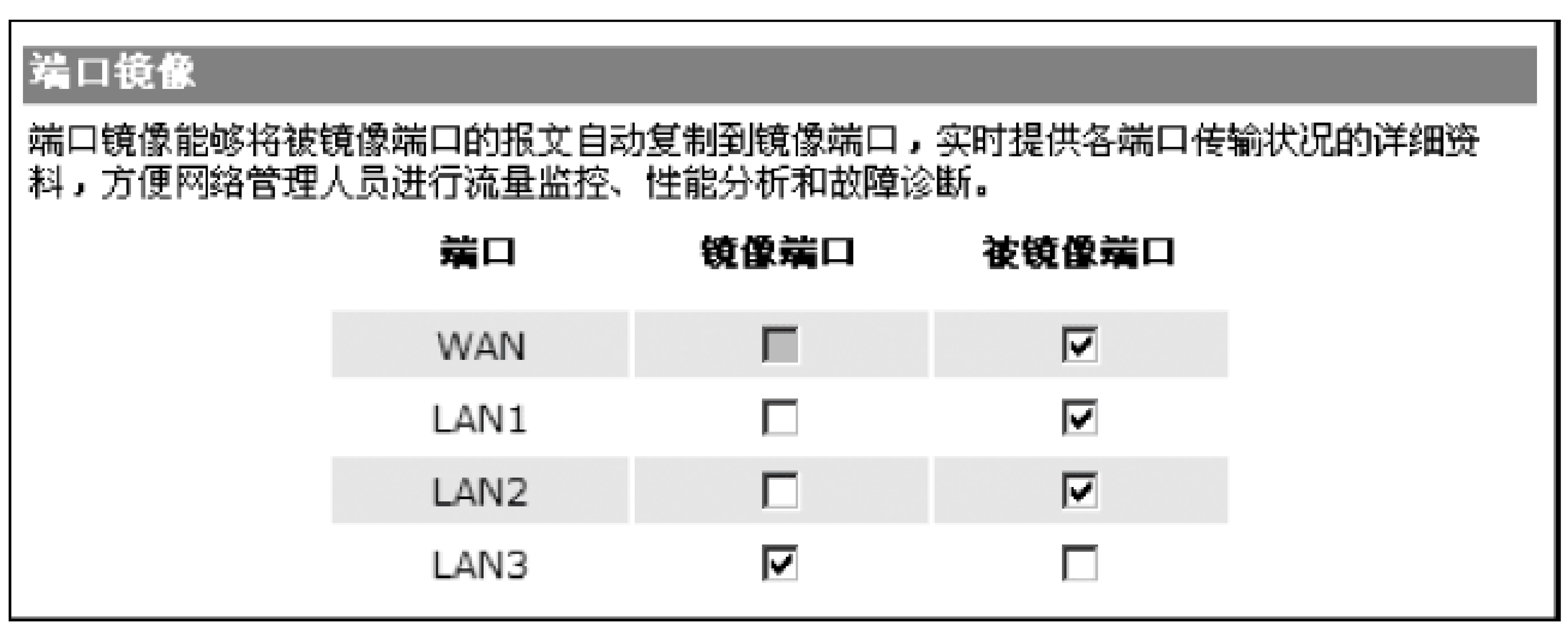


图 4-21　端口镜像

将以上信息收集整理，并详细了解故障现象和网络拓扑后，求助呼叫中心处理。


ER系列路由器忘记密码故障排查
表示上一步结果正常
表示上一步结果出现问题
向健民
开始
是否可进入Web登录页面
输入密码错误时是否有密码提示
通过Console口恢复
通过密码提示找回
通过页面中忘记密码恢复
拨打热线
400-810-0504
寻求帮助

1. 开始

ER 系列路由器一般采取 Web 方式登录和管理，其 Console 端口提供设备在 Web 无法登录或 Web 忘记账号密码时应急恢复的功能。所以定位故障的思路为：先判断是否能进入 Web 登录页面，然后尝试是否能够通过“密码提示”找回密码，最后需通过 Console 口进行恢复。

2. 流程图相关操作说明

(1) 是否可进入 Web 登录页面

输入 ER 路由器的 Web 登录地址，查看是否可以进入 Web 登录页面，如图 4-22 所示是 ER3108GW 通过 http://192.168.1.1 登录的首页。



图 4-22 Web 登录页面

说明：

① Web 页面无法显示，请更换不同浏览器尝试登录！

② ER 路由器 Web 登录地址可以通过以下方式获取。

- ER 路由器的默认的登录地址为 http://192.168.1.1，可尝试以此默认地址登录。
- 在 ER 路由器 LAN 接口下，管理 PC DHCP 获取的网关地址一般为 ER 路由器的 Web 登录地址。如图 4-23 所示，管理 PC 本地连接的默认网关为 10.165.16.1，可尝试以此默认网关 http://10.165.16.1



图 4-23 默认网关

登录。

- 在 ER 路由器 LAN 接口下，管理 PC DHCP 无法获取地址，可尝试 Console 口下输入 *ip address* 命令并回车，如下所示，即可显示路由器 LAN 口的 IP 地址，通过手工设置 PC 的默认网关地址登录。

```
<H3C>ip address
The LAN interface information:
  IP address: 192.168.1.1
  Mask: 255.255.255.0
```

（2）输入密码错误时是否有密码提示

ER 路由器 Web 登录页面上输入默认的用户名和密码 admin/admin，尝试是否可以登录，用户密码错误，是否出现密码提示，如图 4-24 所示。

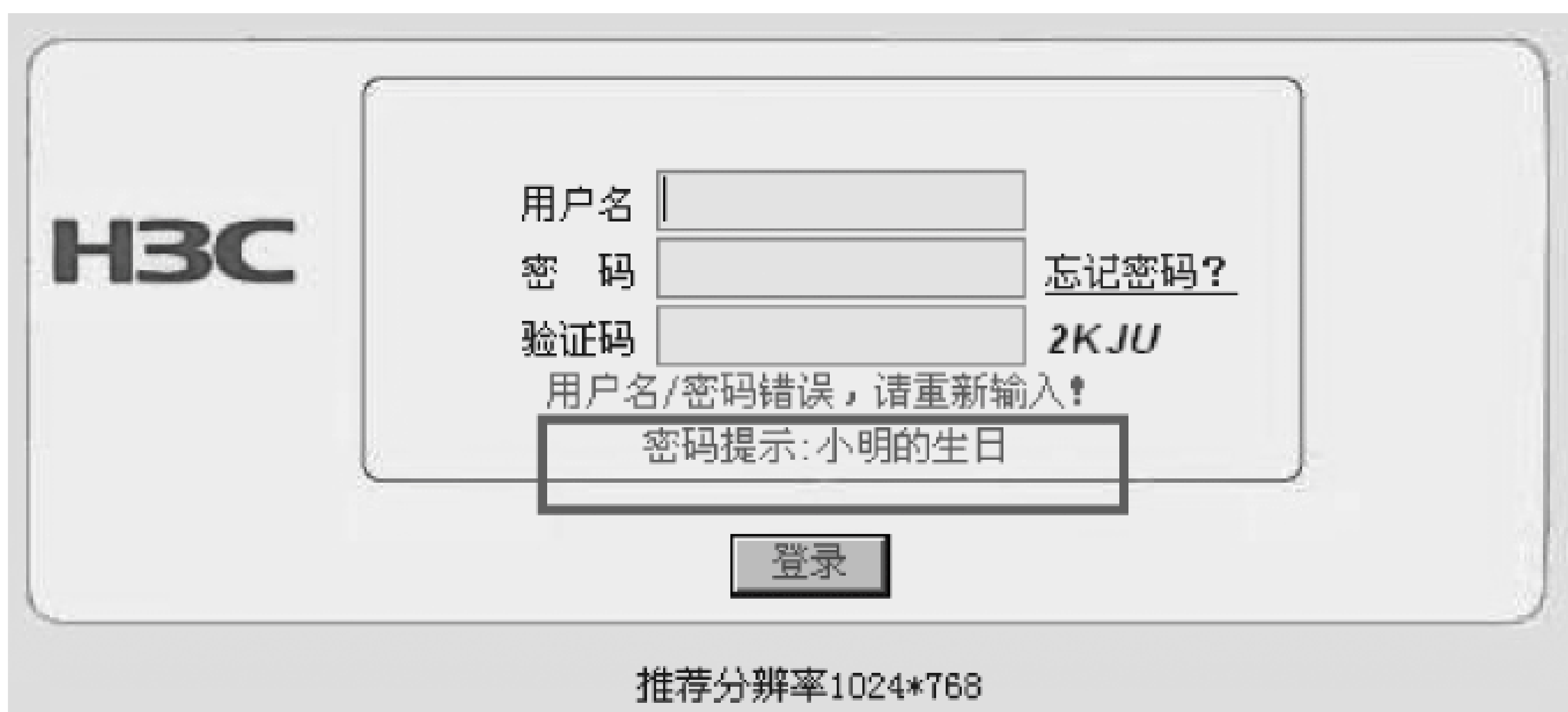


图 4-24　输入密码错误提示

说明：

① 登录用户名为 admin，密码区分大小写，支持 1～31 位英文状态下的字符。

② 如果页面没有“密码提示”信息，则可能的原因如下。

- ER 路由器软件版本非最新版本，此版本不具备“密码提示”功能。
- 设置登录用户名密码时，未在密码管理内设置密码提示内容，如图 4-25 所示。

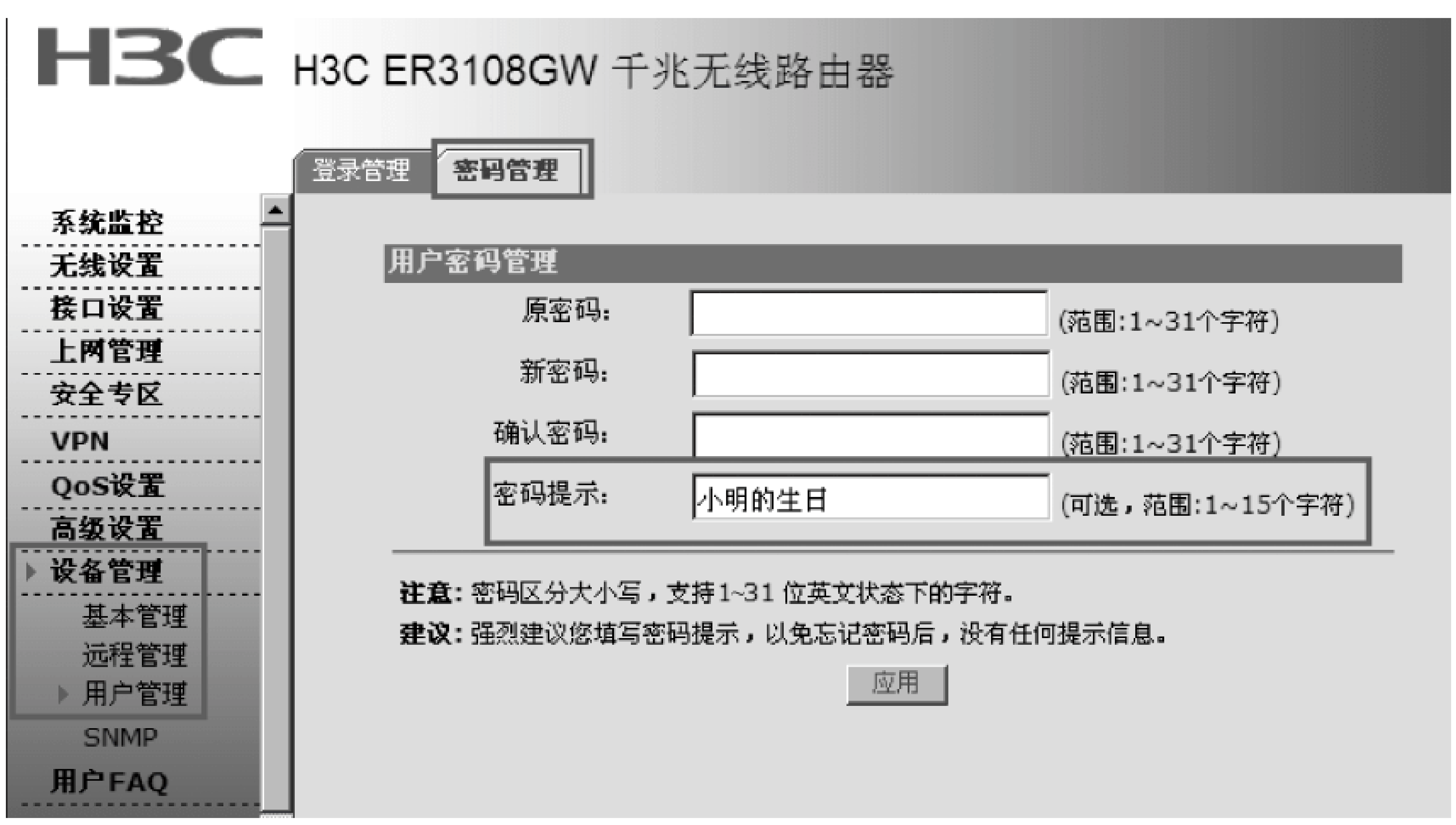


图 4-25　未设置密码提示内容时

(3) 通过 Console 口恢复

当 ER 路由器无法登录到 Web 页面,可通过 Console 方式登录 ER 路由器进行命令行方式恢复。

① 通过串口登录命令行界面,通过 password 命令来设置新密码。

命令:*password*

```
<H3C>password
Changing password for admin
Enter the new password (minimum of 1, maximum of 31 English characters)
Enter new password:
Re-enter new password:
Password has been set successfully.

<H3C>
```

② 如果 password 命令需要输入原密码,则只能输入 restore default 命令恢复到出厂设置

说明:恢复出厂设置后,路由器的用户名、密码以及 IP 地址等所有设置都会被恢复到默认设置。

命令:*restore default*

```
<H3C>password
Changing password for admin
Old password:
Incorrect password for admin.
<H3C>restore default
This command will restore the default configuration and reboot the system.
The current configuration will be lost if you continue.
Continue? [Y/N]Y
<H3C>
```

管理 PC 串口连接 ER 路由器方法如下。

① 通过配置线缆(DB-9 转成 RJ45 的通用转换线)连接到计算机,如图 4-26 所示。

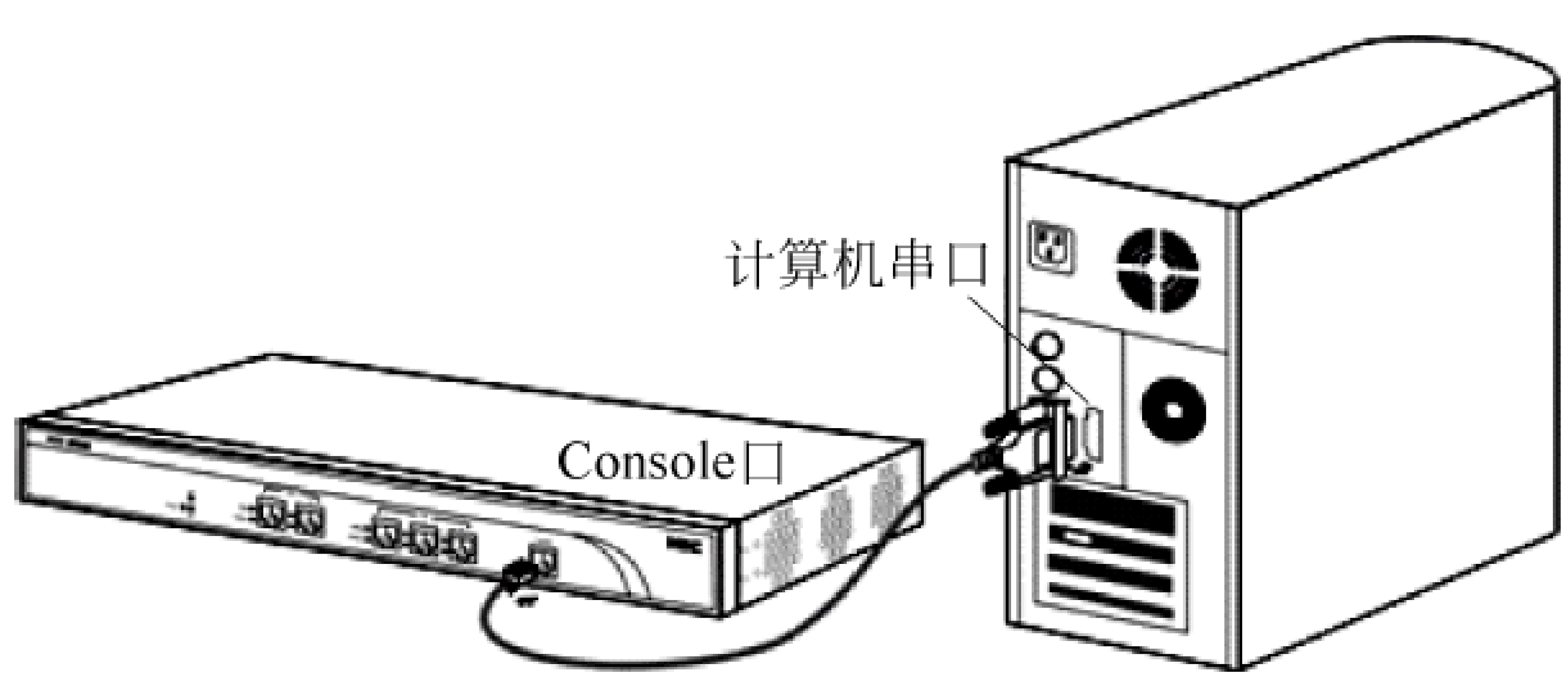


图 4-26 连接计算机

② 配置管理计算机参数,以 Windows XP 附带的超级终端为例,打开管理计算机,在管理计算机 Windows 界面上单击"开始"→"所有程序"→"附件"→"通讯"命令,运行终端仿真程序。在"名称"文本框中键入新建连接的名称,比如:aaa,如图 4-27 所示,单击"确定"按钮。

③ 在“连接时使用”下拉框中选择进行连接的串口(请确保选择的串口应与配置线缆实际连接的串口相一致),单击“确定”按钮,如图 4-28 所示。



图 4-27　连接描述

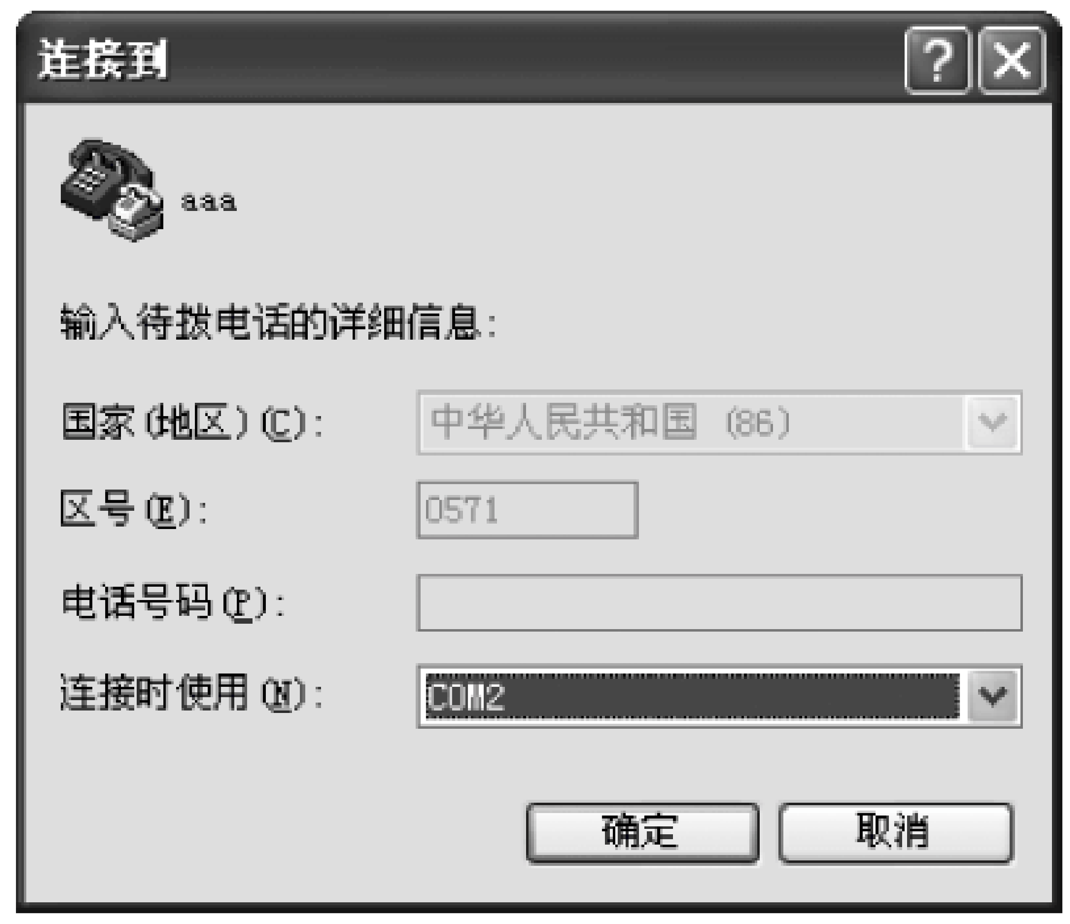


图 4-28　选择串口

④ 在串口的属性对话框中设置相关参数,需注意,每秒位数(波特率):9600,数据流控制:无。单击“确定”按钮,如图 4-29 所示。

⑤ 单击“文件”→“属性”→“设置”命令,进入如图 4-30 所示的属性设置窗口。选择“终端仿真类型”为“自动检测”,单击“确定”按钮。



图 4-29　串口属性对话框



图 4-30　属性设置窗口

⑥ 按 Enter 键后,即可登录路由器,且终端上显示命令行提示符＜H3C＞,如图 4-31 所示。

(4) 通过密码提示找回

通过 ER 路由器的密码提示功能,根据密码提示信息找回登录密码。如图 4-32 所示,密码提示为“小明的生日”。

(5) 通过页面中忘记密码恢复

通过单击 ER 路由器的登录页面“忘记密码?”链接,通过链接内容“忘记密码怎么办”,通过串口恢复到出厂设置,如图 4-33 所示。

说明:恢复出厂设置后,路由器的用户名、密码以及 IP 地址等所有设置都会被恢复到默认设置。

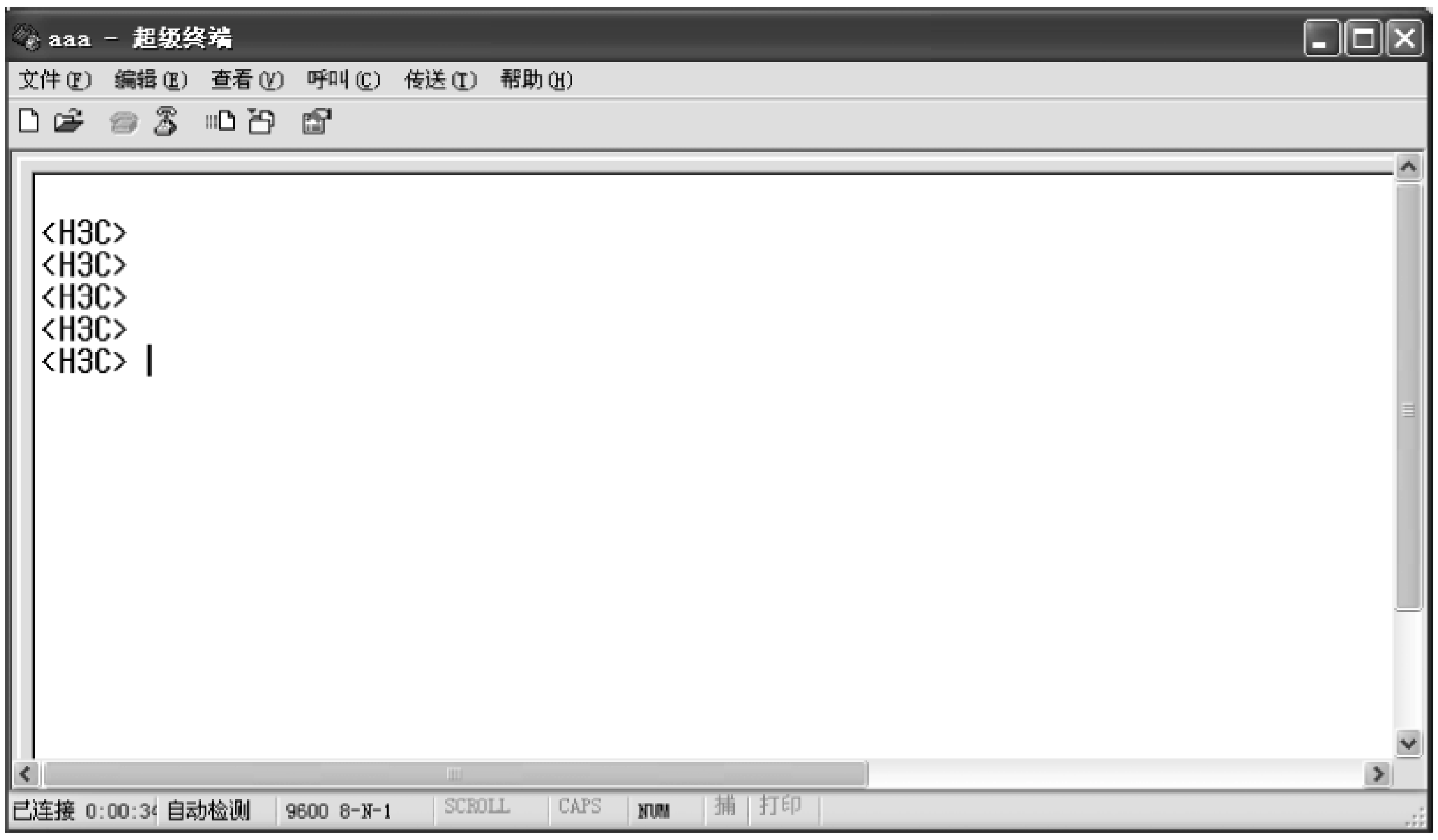


图 4-31　超级终端

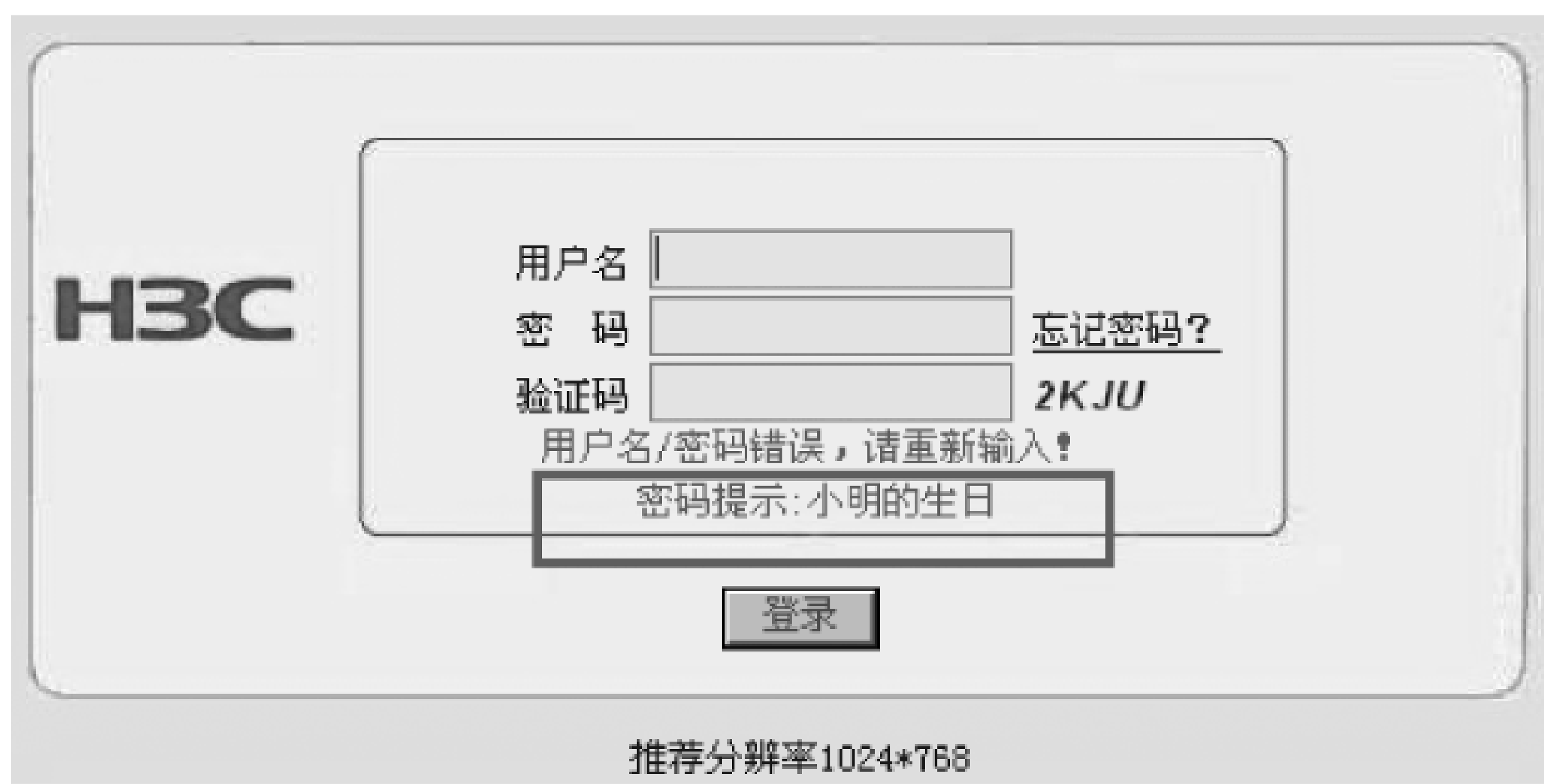


图 4-32　密码提示

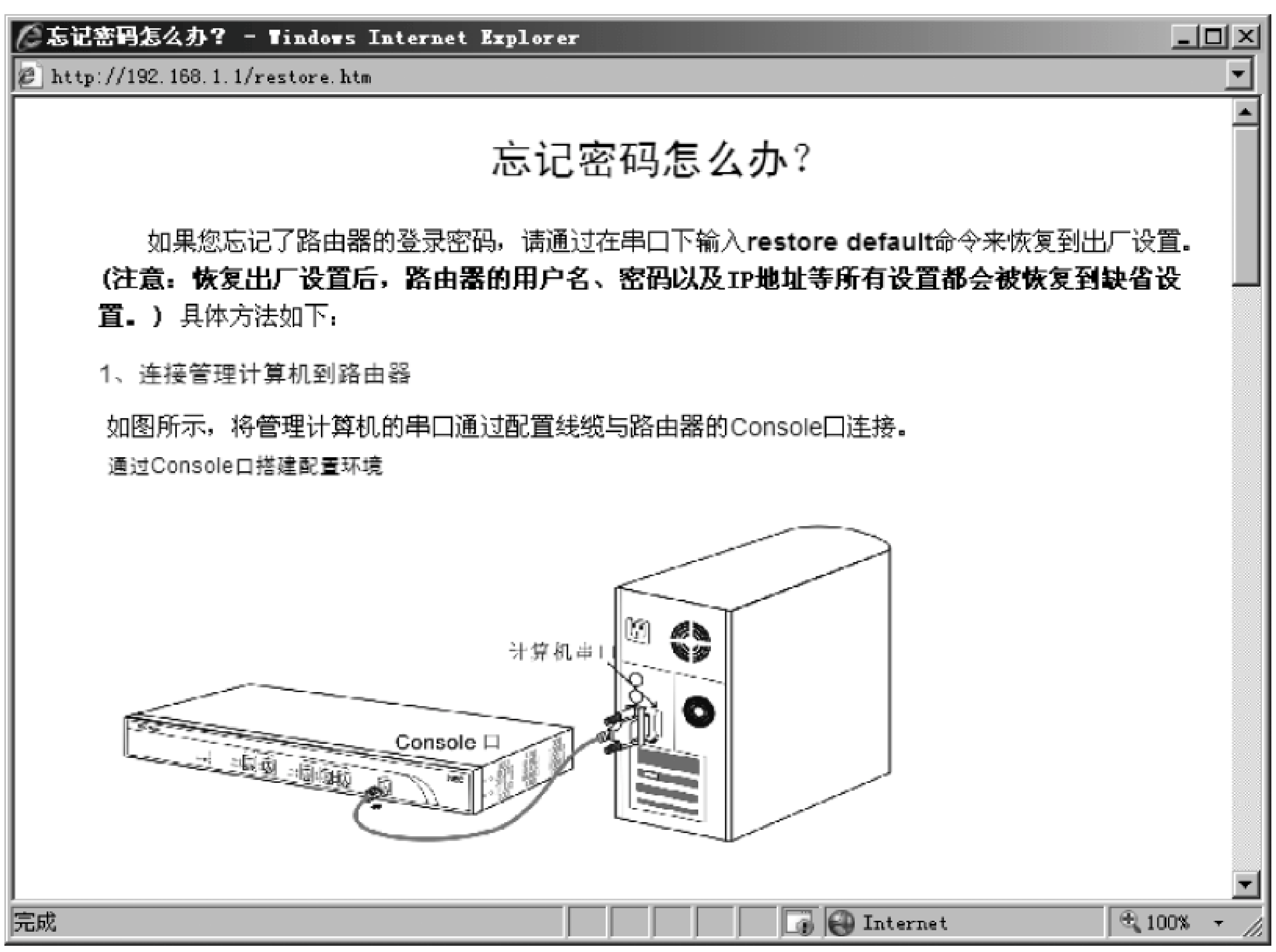


图 4-33　忘记密码怎么办

05

交换机产品


高端产品电源故障排查
张 辛
表示上一步结果正常
表示上一步结果出现问题
电源问题排查
查看电源监控模块和电源模块指示灯状态
查看日志告警信息和电源状态
交叉验证
收集信息
拨打热线
400-810-0504
寻求帮助

1. 开始

电源系统由硬件和软件两部分构成，所以定位故障的思路是：先查硬件、再查软件；先查外部供电，再查电源模块。

2. 流程图相关操作说明

(1) 查看电源监控模块和电源模块指示灯状态

电源监控模块和电源模块指示灯可直接反应电源的运行状态，查硬件问题请先查看电源监控模块（S12500 和 CR16000 特有）和电源模块指示灯状态。

电源监控模块指示灯状态如表 5-1 所示。

表 5-1 电源监控模指示灯状态

<table>
<tr><th>指示灯名称</th><th>颜色</th><th>状态</th><th>含　义</th></tr>
<tr><td rowspan="2">RUN</td><td rowspan="2">绿色</td><td>灯常亮</td><td>表示电源监控模块正常工作</td></tr>
<tr><td>灯灭</td><td>表示电源监控模块有故障</td></tr>
<tr><td rowspan="3">MAJOR</td><td rowspan="3">红色</td><td>灯常亮</td><td>包括但不限于以下 4 种情况：
① 表示电源模块有故障
② 电源框内所有电源模块被拔出
③ 电源框开关关闭
④ 电源模块在位，但未接入交流电</td></tr>
<tr><td>灯先亮后灭</td><td>表示插拔电源模块</td></tr>
<tr><td>灯灭</td><td>表示电源模块正常工作</td></tr>
<tr><td>MINOR</td><td>黄色</td><td>灯灭</td><td>保留</td></tr>
</table>

电源模块指示灯状态如表 5-2 所示。

表 5-2 电源模块指示灯状态

<table>
<tr><th>指示灯名称</th><th>颜色</th><th>状态</th><th>含　义</th></tr>
<tr><td rowspan="3">电源输入指示灯</td><td rowspan="3">绿色</td><td>灯常亮</td><td>表示电源输入正常</td></tr>
<tr><td>灯灭</td><td>表示电源没有输入</td></tr>
<tr><td>灯闪烁</td><td>表示电源输入超过最大范围</td></tr>
<tr><td rowspan="3">电源输出指示灯</td><td rowspan="3">绿色</td><td>灯常亮</td><td>表示电源模块输出正常</td></tr>
<tr><td>灯灭</td><td>表示电源模块没有输出</td></tr>
<tr><td>灯闪烁</td><td>表示电源模块输出过载</td></tr>
<tr><td rowspan="2">过温告警指示灯</td><td rowspan="2">黄色</td><td>灯常亮</td><td>表示电源模块过温告警</td></tr>
<tr><td>灯灭</td><td>表示电源模块正常工作</td></tr>
<tr><td rowspan="2">电源故障指示灯</td><td rowspan="2">红色</td><td>灯常亮</td><td>表示电源模块出现故障</td></tr>
<tr><td>灯灭</td><td>表示电源模块正常工作</td></tr>
</table>

(2) 依据指示灯状态做交叉验证

依据上述指示灯状态列表，如果指示灯状态有异常，请根据指示灯状态，通过交叉验证确认故障所在，方法如下。

CR16000、S12500 的电源监控模块 RUN 灯灭、MAJOR 灯亮，表示电源模块有故障，请进一步查看电源模块指示灯状态。

① 如果电源模块输入指示灯灭，表示电源输入有问题，请交叉电源模块对应的电源线和供电线路，确认供电线路有无问题。如果现场不具备交叉验证的条件，请联系机房管理员进行检查确认。

② 如果电源模块输入指示灯正常，输出指示灯灭，表示电源输出有问题，请交叉电源模块，确认故障是否跟随电源模块走；跟随电源模块走，则为电源模块故障，否则为电源框故障。如果现场不存在交叉验证的条件，请按照后续步骤收集信息，拨打 400-810-0504 寻求帮助。

SR8800、S9500E、S9500 和 S8500 直接查看电源模块指示灯状态。

① 如果电源模块输入指示灯灭，表示电源输入有问题，请交叉电源模块对应的电源线和供电线路，确认供电线路有无问题。如果现场不具备交叉验证的条件，请联系机房管理员进行检查确认。

② 如果电源模块输入指示灯正常，输出指示灯灭，表示电源输出有问题，请交叉电源模块，确认故障是否跟随电源模块走；跟随电源模块走，则为电源模块故障，否则为电源框故障。如果现场不存在交叉验证的条件，请按照后续步骤收集信息，拨打 400-810-0504 寻求帮助。

以上所有操作请在征得客户同意下进行，并确保设备供电充足，不会对客户业务造成影响。设备功耗计算请参考各产品的安装指导。根据交叉验证的结果确认故障所在，拨打 400-810-0504 寻求帮助。

(3) 查看日志告警信息和电源状态

如果上述操作无法定位故障所在，怀疑系统软件存在问题，请收集设备的诊断信息、日志信息文件和 diagfile 文件，同时拍摄电源状态指示灯，拨打 400-810-0504 寻求帮助。

(4) 收集信息

① 收集设备诊断信息。

命令：*display diagnostic-information*

例如：

```
<H3C>display diagnostic-information
------------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( *.diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

   0     drw-           -   Jul 07 2013 07:16:12    logfile
   1     drw-           -   Jul 07 2013 07:13:04    diagfile
   2     -rw-     4924407   May 06 2013 06:43:32    default.diag
   3     drw-           -   May 02 2013 03:31:52    diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

② 收集设备日志信息文件。

命令：*logfile save*

例如：

```
<H3C>logfile save
------------------------------------------------------------------------
Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

   0     -rw-   10484413   Dec 26 2013 08:37:00    logfile1.log
   1     -rw-     150941   Dec 14 2013 10:10:54    logfile.log
   2     -rw-     127193   Jan 21 2013 09:41:28    logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

③ 收集设备 diagfile 信息文件(SR8800 V3R3 以前版本、S9500、S8500 均没有该文件，不用收集)。

命令：*_diagnose-file save*

例如：

```
[H3C]_h
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]_diagnose-file save
------------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

   0     -rw-    2418760   Jul 09 2013 01:43:16   diagfile1.log
   1     -rw-      69266   Dec 03 2013 09:38:36   diagfile.log
   2     -rw-    4291181   Dec 10 2013 12:27:48   diagfile2.log
   3     -rw-     292979   Jul 07 2013 07:31:52   diagfile3.log
   4     -rw-    5240510   Jul 08 2013 11:55:00   diagfile4.log
   5     -rw-     110346   Jul 07 2013 08:51:44   diagfile5.log
   6     -rw-     192711   Jul 09 2013 12:03:26   diagfile6.log
   7     -rw-     166363   Jul 09 2013 08:38:20   diagfile7.log
   8     -rw-      17121   Jul 08 2013 16:37:48   diagfile8.log
   9     -rw-     101888   Jul 07 2013 07:54:28   diagfile9.log
   10    -rw-    2375568   Jul 09 2013 08:06:34   diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```


高端产品业务板CPU利用率高故障排查
表示上一步结果正常
表示上一步结果出现问题
马 昊
开始
判断CPU利用率是否异常高
确认导致CPU利用率异常高的CPU任务
判断导致CPU利用率异常高的原因，排除异常源
拨打热线
400-810-0504
寻求帮助

1. 开始

正常的业务单板CPU占用率一般都是在30%以内的,OAA单板和功能单板(如NAT单板、NetStream单板等)正常情况下的CPU利用率偏高,不在此云图的排查对象范围内。

2. 流程图相关操作说明

(1) 判断CPU利用率是否异常高

命令:*display cpu*

应根据单板的5分钟内的平均占用率来判断该单板的CPU利用率是否异常;比如在下面的例子中可以判断出3号槽位的单板CPU占用率异常。

```
<H3C>display cpu
Slot 0 CPU usage:
        11% in last 5 seconds
        13% in last 1 minute
        13% in last 5 minutes
Slot 3 CPU usage:
        35% in last 5 seconds
        59% in last 1 minute
        51% in last 5 minutes
```

(2) 确认导致CPU利用率异常高的CPU任务

命令:*display cpu-usage entry-number verbose slot 0*(S9500/S8500不支持)

从最新记录(倒数第一条记录)开始,显示entry-number条记录(下面的举例中是5条)。

```
<H3C>display cpu-usage 5 verbose slot 0
---------- CPU usage info (no:  0  idx: 31) ----------
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage             : 33%                    <--- CPU使用率
CPU Usage Stat. Time  : 2009-07-26  16:55:33   <--- 查看时间
CPU Usage Stat. Tick  : 0x15(CPU Tick High) 0x429be6f6(CPU Tick Low)
Actual Stat. Cycle    : 0x0(CPU Tick High) 0xb2d2a975(CPU Tick Low)

TaskName      CPU       Runtime(CPU Tick High/CPU Tick Low)
VIDL          67%         0/77d02af4
TICK           0%         0/ 469276
…
co0           31%         0/39012f2b
```

从上面的举例中,可以知道是co0任务引起CPU升高的(VIDL是空闲任务),这时就要考虑Console用户进行了什么命令操作才导致的。

(3) 判断导致CPU利用率异常高的原因,排除异常源

常见导致CPU利用率高的任务如下。

① L2AU/L2SY/L2DM/L2HC任务,这些任务都和MAC地址学习相关,需要排查设备是否存在MAC地址漂移,或者设备收到大量TC报文,导致MAC地址频繁刷新。

对于MAC地址漂移问题,需要多次收集ARP表和MAC地址表,进行对比分析排查。

S12500/S9500E R1828 版本及之后版本，可以直接通过 display mac-flapping information 命令查看 MAC 地址迁移记录。

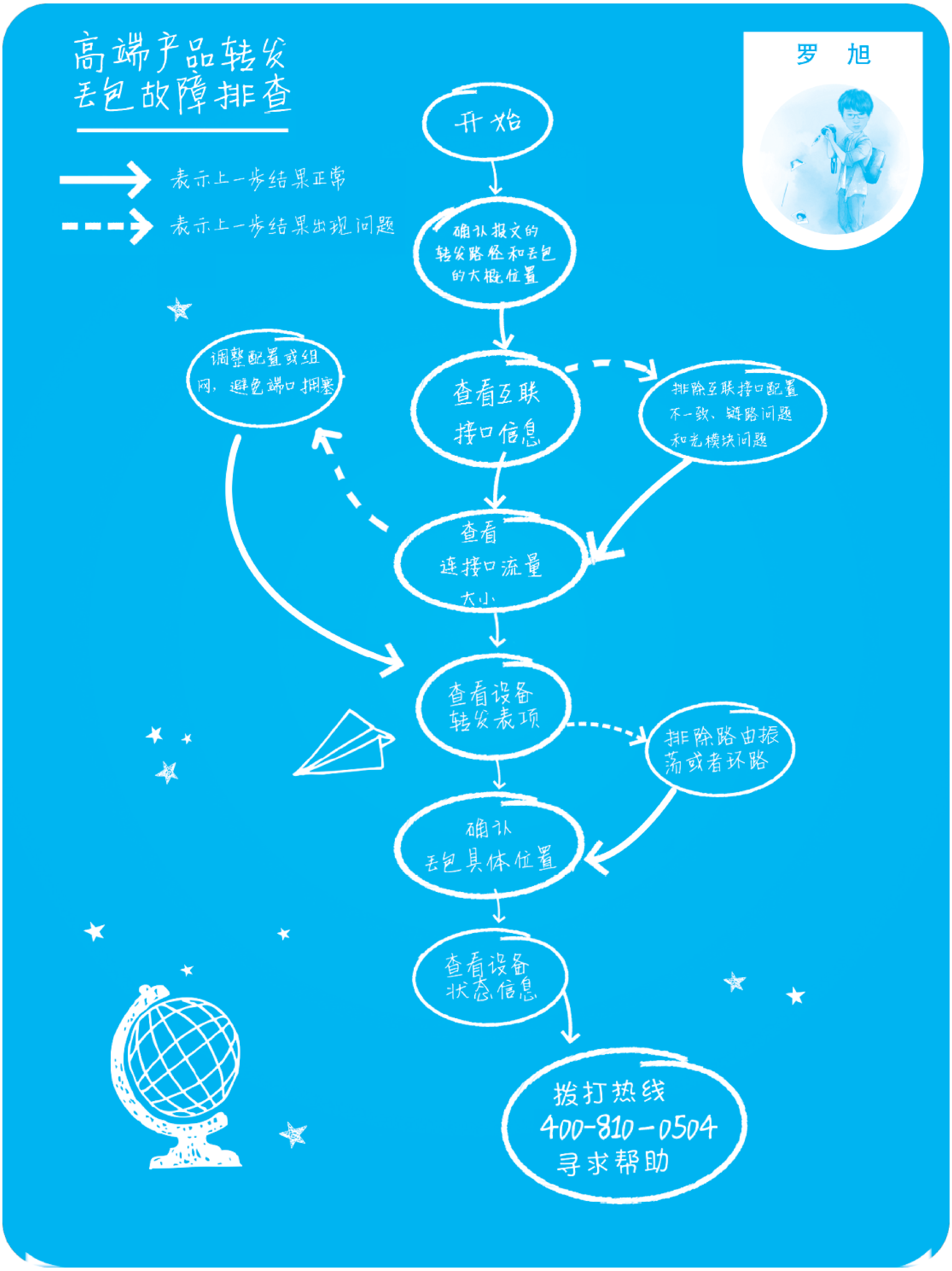
对于设备收到大量 TC 报文问题，设备收到 TC 报文时，会打印日志，根据日志信息可以排查 TC 报文来源。相关日志信息举例如下。

```
H3C MSTP/6/MSTP_NOTIFIED_TC: -Slot=9; Instance 0's port GigabitEthernet9/0/15 was notified of a topology change
```

② ROUT 任务，路由管理任务，需要排查设备是否存在路由振荡问题。通过 display ip routing-table statistics 命令可以查询路由表统计信息，如果路由增删计数变化明显，请排查相关路由协议振荡源。

③ ARP 任务，处理 ARP 协议报文的任务，需要排查是否存在 ARP 攻击问题。通过查看日志信息，可以排查设备是否受到 ARP 攻击。

④ co0 任务，Console 口用户与设备之间的会话任务，需要确认 Console 口用户是否正在收集诊断信息、用复制粘贴方式下发大量配置等操作。如果是其他 CPU 任务，请直接电话咨询 400-810-0504。


高端产品转发丢包故障排查
表示上一步结果正常
表示上一步结果出现问题
罗 旭
开始
确认报文的转发路径和丢包的大概位置
查看互联接口信息
排除互联接口配置不一致、链路问题和光模块问题
调整配置或组网，避免端口拥塞
查看连接口流量大小
查看设备转发表项
排除路由振荡或者环路
确认丢包具体位置
查看设备状态信息
拨打热线 400-810-0504 寻求帮助

1. 开始

转发丢包问题的主要排查思路如下。

① 确认报文的转发路径和丢包的大概位置。

② 查看存在丢包的设备间的互联接口信息，排除互连接口配置不一致、链路问题和光模块问题。

③ 查看互联接口流量大小，调整配置或组网，避免端口拥塞。

④ 查看设备转发表项，排除路由振荡或者环路。

⑤ 通过流量统计或者镜像抓包的方式，确认丢包具体位置。

⑥ 查看设备状态信息，排除设备异常或者收集故障信息并联系400寻求帮助。

2. 流程图相关操作说明

(1) 确认报文的转发路径和丢包的大概位置

对于丢包问题，首先要确认报文的转发路径和丢包的大概位置，缩小排查范围。

① 通过 tracert 或者查看设备路由表或者查看网络拓扑图的方式，确认报文转发路径；

② 在终端上依次 ping 转发路径上的网络设备，如果发现 ping A 设备不丢包，但是 ping 下一跳 B 设备丢包，则可以初步确认 A 设备，或者 B 设备，或者 A 设备和 B 设备之间的链路上存在转发丢包。

(2) 查看互连接口信息

确认了丢包的大概位置后，首先查看相关设备的互联接口信息，确认是否是接口存在错包导致网络丢包。通过命令行查看接口下看是否存在 errors、frame、crc 校验等错误计数，通过多次查看，看该计数是否在不断增加。

命令：*display interface GigabitEthernet 3/0/1*

例如：多次查看该命令，可以确认互连接口 3/0/1 有收到错包，且在不断增长。

```
<H3C>display interface GigabitEthernet 3/0/1
GigabitEthernet3/0/1 current state: Up
Line protocol current state: Up
…
Input:23805421 input errors, 0 runts, 0 giants, 0 throttles
          1386 CRC, 23804035 frame, 0 overruns, - aborts
          0 ignored, - parity errors
```

对于 SDH 线路，同样可以查看接口下有无错包，还可以查看接口下有无相关链路层告警等。

```
Serial3/0/1/6:0 current state: Up
Line protocol current state: Up
…
Input(total):  27616419 packets,  2996528783 bytes
Input(Bad):120 Abort,  231 FCS-Error,  0 FIFO-Abort,  0 Giant,  0 Runt
Output(total):  18171442 packets,  6872764415 bytes
```

(3) 检查配置，替换测试

如果接口下存在错包计数，且在不断增加，可能是接口配置不一致、传输异常、光模块异常等原因导致，可以通过如下调整配置或者通过替换测试排查解决。

① 接口下配置不一致。检查互连接口的配置，看两端双工模式是否一致、封装模式是否一致，如果不一致则将两端修改为一致。

② 传输异常。传输质量差，或者中间传输设备异常也会导致设备接口下出现错包。可通过更换尾纤、链路等方式进行排查测试。对于电口，可更换网线、端口等方式进行排查测试。

③ 光模块异常。如果设备通过光口互连，可通过如下命令判断光模块是否存在异常告警，光模块收发光功率是否异常。如果是，可替换光模块后再进行业务测试。

命令：*display transceiver diagnosis interface GigabitEthernet 3/0/1*

display transceiver alarm interface GigabitEthernet 3/0/1

例如：通过命令查看，可以发现本端光模块发光功率明显偏低，超出临界值，且光模块有发光过低的告警。

```
<H3C>display transceiver diagnosis interface GigabitEthernet 3/0/1
GigabitEthernet3/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    32        3.37        11.46     -12.19         -35.19
<H3C> display transceiver alarm interface GigabitEthernet 3/0/1
GigabitEthernet3/0/1 transceiver current alarm information:
  TX power low
```

排除问题后，通过 ping 测试看丢包现象是否还存在。

(4) 查看互连接口流量大小

如果接口下没有持续增长的错包或者没有告警等，可能是接口下流量过大或者存在限速，接口下发生拥塞导致丢包。

可以通过查看互连接口下流量大小，查看接口下是否存在限速或者流量整形等配置进行确认。另外如果接口下广播流量特别大，则可能存在环路。

命令：*display interface GigabitEthernet 3/0/1*

display qos policy interface gigabitethernet 3/0/1 inbound

例如：查看接口下配置可以发接口下配置了限速，且接口下流量较大，通过命令可查看到接口下有拥塞丢包计数。

```
<H3C>display interface GigabitEthernet 3/0/1
GigabitEthernet6/1/1 current state: Up
Line protocol current state: Up
…
Last 300 seconds input:154690 packets/sec 50590840 bytes/sec   83%
Last 300 seconds output:74280 packets/sec 101038610 bytes/sec  42%
…
#
<H3C> display qos policy interface gigabitethernet 3/0/1 inbound
   Interface: GigabitEthernet3/0/1
   Direction: Inbound
   Policy: H3C
   Classifier: H3C
```

```
          Operator: AND
          Rule(s) : If-match acl3000
          Behavior: H3C
           Committed Access Rate:
             CIR 1000 (kbps), CBS 100000 (byte), EBS 0 (byte)
             Red Action: discard
             Green :51111(Packets) 0(Bytes)
             Yellow: 0(Packets) 0(Bytes)
             Red    : 322(Packets) 0(Bytes)
```

(5) 调整配置或组网,避免端口拥塞

如果通过上一步确认是因为存在限速或者流量过大等原因导致丢包,可根据现场实际情况进行调整解决。如和客户协调后,取消限速先关策略或适当增大限速速率、通过链路聚合来增大互连带宽,或者将部分流量迁移到其他端口等方法来避免互连接口下出现拥塞。

调整之后,通过 ping 测试看丢包现象是否还存在。

(6) 查看设备转发表项

如果接口下没有错报,而且流量较小或者未超过限速,则可能是设备的转发表项存在异常导致丢包。可通过多次查看设备路由表、ARP 表和 MAC 表等转发表项看是否正常,如果表项存在异常肯定会影响报文转发。

命令:*display arp all* | *include 10.1.1.1*

例如:通过命令查看,可以确认去往 10.1.1.1 的报文从 G3/0/1 接口学到,多次查看该表项,发现该 arp 发生了漂移。

```
     <H3C> display arp all | include 10.1.1.1
                   Type: S-Static    D-Dynamic    A-Authorized
     IP Address      MAC Address     VLAN ID      Interface        Aging Type
     10.1.1.1        000f-e283-4c98  N/A          GE3/0/1            N/A   D
     <H3C> display arp all | include 10.1.1.1
                   Type: S-Static    D-Dynamic    A-Authorized
     IP Address      MAC Address     VLAN ID      Interface        Aging Type
     10.1.1.1        000f-e283-4c98  N/A          GE3/0/10           N/A   D
```

(7) 排除路由振荡或者环路

通过多次查看各转发表项,如果发现路由时有时无、路由振荡或者 ARP 漂移等现象,需要对该设备和相关链路进行排查。

对于路由振荡,可查看相应链路、协议状态是否稳定,可通过 debug 等方式测试设备相应协议报文收发包情况是否正常,可参考相关协议云图进行排查;对于环路问题需要根据相应接口逐步排查相应下连设备,排除环路。

在排除了环路或者路由振荡等异常后,再通过 ping 测试看丢包现象是否还存在。

(8) 确认丢包具体位置

如果各转发表项都是正常的,则需要确认丢包发生的具体位置,如某台设备或者某条链路上,再对其进行重点排查。

通过第一步排查步骤已经确认了丢包的大概位置,再在这几台设备的互联接口上做流量统计,来确认丢包发生在具体某台设备或者某条链路上。

SR8800 产品的流量统计配置参考如下,其他产品请参考相应产品的 QoS 配置指导。

```
acl number 3000
 rule0 permit ip source 10.1.1.1 0 destination 20.1.1.1 0
 #
traffic classifier H3C
 if-match acl 3000
 #
traffic behavior H3C
 accounting packet
 #
qos policy H3C
 classifier H3C behavior H3C
 #
interface GigabitEthernet3/0/1
 qos apply policy H3C inbound
 #
```

命令：*display qos policy interface g3/0/1*

例如：终端总共 ping 了 1000 个测试报文，且在上一级设备出方向也正常统计到 1000 个报文，在本设备，通过如下命令查看可以确认设备的 g3/0/1 口只有收到 990 个测试报文，则可判断报文丢在中间传输设备或者传输链路上。

```
<H3C>display qos policy interface g3/0/1
Interface: GigabitEthernet3/0/1
  Direction: Inbound
  Policy: statistic
   Classifier: statistic
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: statistic
      Accounting Enable:
        990 (Packets)
```

如果丢包发生在传输链路上，需要协调排查传输设备或者链路，如果丢包发生在网络设备上，则根据如下情况继续排查。

① 丢包发生在 CPU 转发设备上，如 MSR、SR6600 等设备，请按照后续步骤进一步查看该设备自身的状态信息是否正常。

② 丢包发生在硬件转发设备上，如 S12500、SR88、S5500 等设备，分为以下两种情况。

情况 1：出现丢包的报文，在设备上只是做转发，即报文不上 CPU 处理，这种情况属于设备硬件转发丢包，可直接收集设备故障信息再拨打热线 400-810-0504 寻求帮助。

情况 2：出现丢包的报文，是需要设备 CPU 处理的报文，例如，与设备接口地址互通的报文，请按照后续步骤进一步查看该设备自身的状态信息是否正常。

如果设备存在流量统计的限制，比如无法统计到出方向的转发报文数，则可以使用镜像抓包的方式来确认具体丢包位置。如果现场无法实施镜像抓包，请拨打热线 400-810-0504 寻求帮助。

(9) 查看设备状态信息

通过上一步确认了丢包发生的具体设备，可查看该设备的运行状态和日志信息，可能因为设备 CPU 高、设备受到攻击、转发错误等原因导致丢包，排查方法如下。

① 查看该设备的 CPU 利用率。如果设备 CPU 利用率较高，则可能因为 CPU 任务忙，影

响某些 CPU 转发设备或者需要 CPU 处理的硬件转发设备的报文转发，即可能导致丢包，可参考 CPU 利用率高问题处理的云图进行排查。

② 查看设备日志信息。如果设备日志中存在异常告警，如受到攻击等，也可能会导致设备丢包。需要通过设备打印的 IP/MAC 地址，或者通过抓包确认攻击源进行隔离解决。

③ 如果设备存在设备转发异常等告警信息，可直接收集设备故障信息再拨打热线 400-810-0504 寻求帮助。

如果设备存在丢包，但未发现设备上述异常，或者上述异常解决后还存在丢包，可收集设备故障信息再拨打热线 400-810-0504 寻求帮助。

命令：*display cpu-usage*

例如：通过命令查看，确认设备当前 CPU 利用率较高，可能影响设备的报文处理。

```
<H3C> dis cpu-usage
Slot 0 CPU usage:
        42% in last 5 seconds
        45% in last 1 minute
        43% in last 5 minutes
Slot3 CPU usage:
        53% in last 5 seconds
        56% in last 1 minute
        55% in last 5 minutes
```

命令：*display logbuffer reverse*

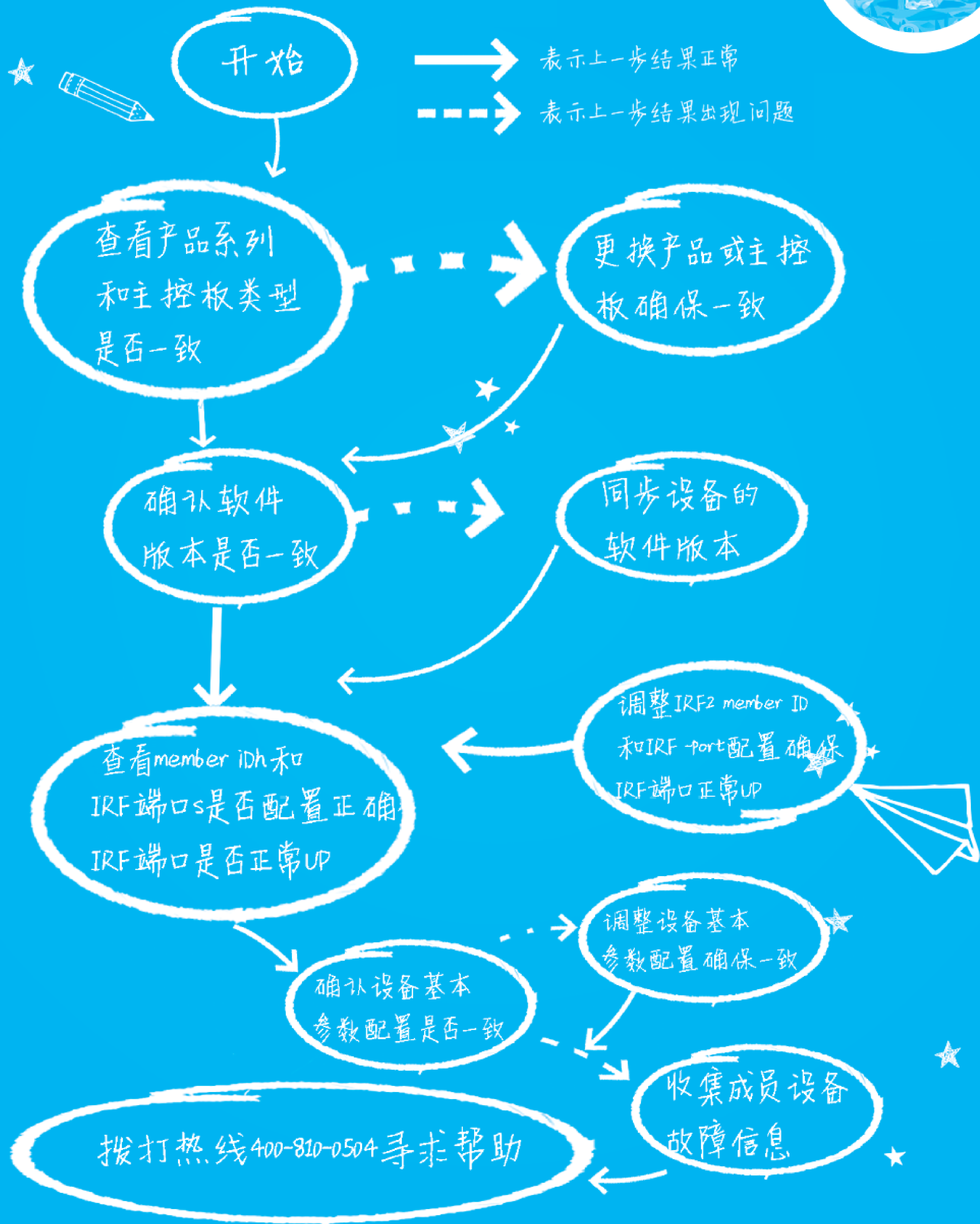
例如：通过命令查看，确认异常时，设备受到 ARP 攻击，可能导致设备相关 ARP 时有时无。

```
May 22 10:31:35 2013 S9512 DIAGCLI/5/LOG_WARN:Slot=3;
 Detect ARP attack from MAC d43d-7e46-b542, VLAN: 200, GigabitEthernet3/0/18 !
May 22 10:31:46 2013 S9512 DIAGCLI/5/LOG_WARN:Slot=3;
 Detect ARP attack from MAC 0040-4848-ed68, VLAN: 100, GigabitEthernet3/0/1 !
```

高端产品IRF2堆叠无法建立故障排查

关 萌





1. 开始

由于 IRF2 堆叠是将多台设备虚拟成一台设备的技术，设备的一些基本参数一定要保证一致。所以定位故障的思路如下。

① 硬件参数一致性：包括产品系列和主控板。

② 软件版本一致性，IRF2 要求软件版本完全一致。

③ IRF2 的 member ID 和 IRF-port 对应关系是否正确。

④ 设备其他硬件参数是否一致。

2. 流程图相关操作说明

(1) 查看产品系列主控板类型是否一致

由于 IRF2 堆叠是将多台设备虚拟成一台设备的技术，所以设备的一些基本参数一定要保证一致，首先需要排查硬件一致性。

同一产品系列的产品可以形成 IRF2，不同系列的产品不能形成 IRF2（如 S12508 和 S12518 可以形成 IRF(2) S9508E 和 S12508 不能形成 IRF2)。

查看成员设备主控板类型是否一致。S12500/CR16000 在建立 IRF2 前，请确保组成 IRF 的 S12500/CR16000 使用的主控板丝印完全相同，否则不能形成 IRF2。S9500E 有两类主控板，要求主控板类型一致才能建立堆叠。如：以 B1 作为后缀名的主控板 LSR1SRP2B1 的设备和以 C1 作为后缀名的主控板 LSR1SRP2C1 设备之间不能形成 IRF，但是以 C1 作为后缀名的主控板 LSR1SRP2C1 的设备和以 C2 为后缀名的主控板 LSR1SRP2C2 的设备之间可以形成 IRF。

命令：*display device*

例如：通过命令查看，可以确认本设备主控板类型为 LSR1SRP2C2。

```
<H3C>display device
Slot No.    Brd Type       Brd Status    Software Version
 0          LSR1SRP2C2     Master        S9500E-CMW520-R1825P01
```

(2) 确认软件版本是否一致

由于 IRF2 堆叠是将多台设备虚拟成一台设备的技术，所以设备的一些基本参数一定要保证一致，只有版本完全一致才能形成 IRF2。

分别查看 IRF 成员设备的软件版本是否一致。

命令：*display version*

例如：通过命令查看，可以确认这台设备的版本为 Release 1825P01。

```
<H3C>display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 1825P01
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S12508 uptime is 0 week, 3 days, 0 hour, 22 minutes
```

（3）查看成员设备 IRF 端口和 Member ID 是否配置正确，端口是否正常 Up

S12500 最多支持 4 台设备形成 IRF2，CR16000 最多支持两台设备形成 IRF2，S9500E 最多支持两台设备形成 IRF2。

为了保证成员设备间能正常通信，需要成员设备 IRF 端口 1 连接另一成员设备 IRF 端口 2。为了保证成员设备间端口号等不发生冲突，成员设备的 Member ID 必需不同。

命令：*display irf configuration*

display interface GigabitEthernet1/2/0/1

例如：通过命令查看，可以确认本设备 Member ID 为 1；IRF-Port1 包含的物理端口为 GigabitEthernet1/2/0/1，当前状态为 Up。

```
<H3C>display irf configuration
MemberID Priority IRF-Port1                    IRF-Port2
1        1        GigabitEthernet1/2/0/1       disable

<H3C>display interface GigabitEthernet1/2/0/1
GigabitEthernet1/2/0/1 current state: Up
```

（4）确认成员设备基本配置是否一致

由于 IRF2 堆叠是将多台设备虚拟成一台设备的技术，所以设备的一些基本参数一定要保证一致，设备的硬件运行方式、转发方式等要求一致，包括：系统工作模式、ACL 硬件模式、MPLS VPN POPGO 模式、Portal 用户迁移功能、IRF 增加功能。

命令：*display system working mode*

display acl mode

display vpn label operation

display portal-roaming

display acl ipv6 inbound

[H3C]display this

例如：通过命令查看。

```
<H3C>display system working mode
Current system working mode        : Routee
Working mode after system restart: Routee
Notice: Changing working mode will take effect only after system restart.

<H3C>display acl mode
Current ACL mode                   : advanced
ACL mode after system restart: advanced
Notice: Changing ACL mode will take effect only after system restart.

<H3C>display vpn label operation
  Pop VPN label and look up FIB entry.

<H3C>display portal-roaming
Current portal-roaming             : enable
portal-roaming after system restart: enable
Notice: Changing portal-roaming will take effect only after system restart.

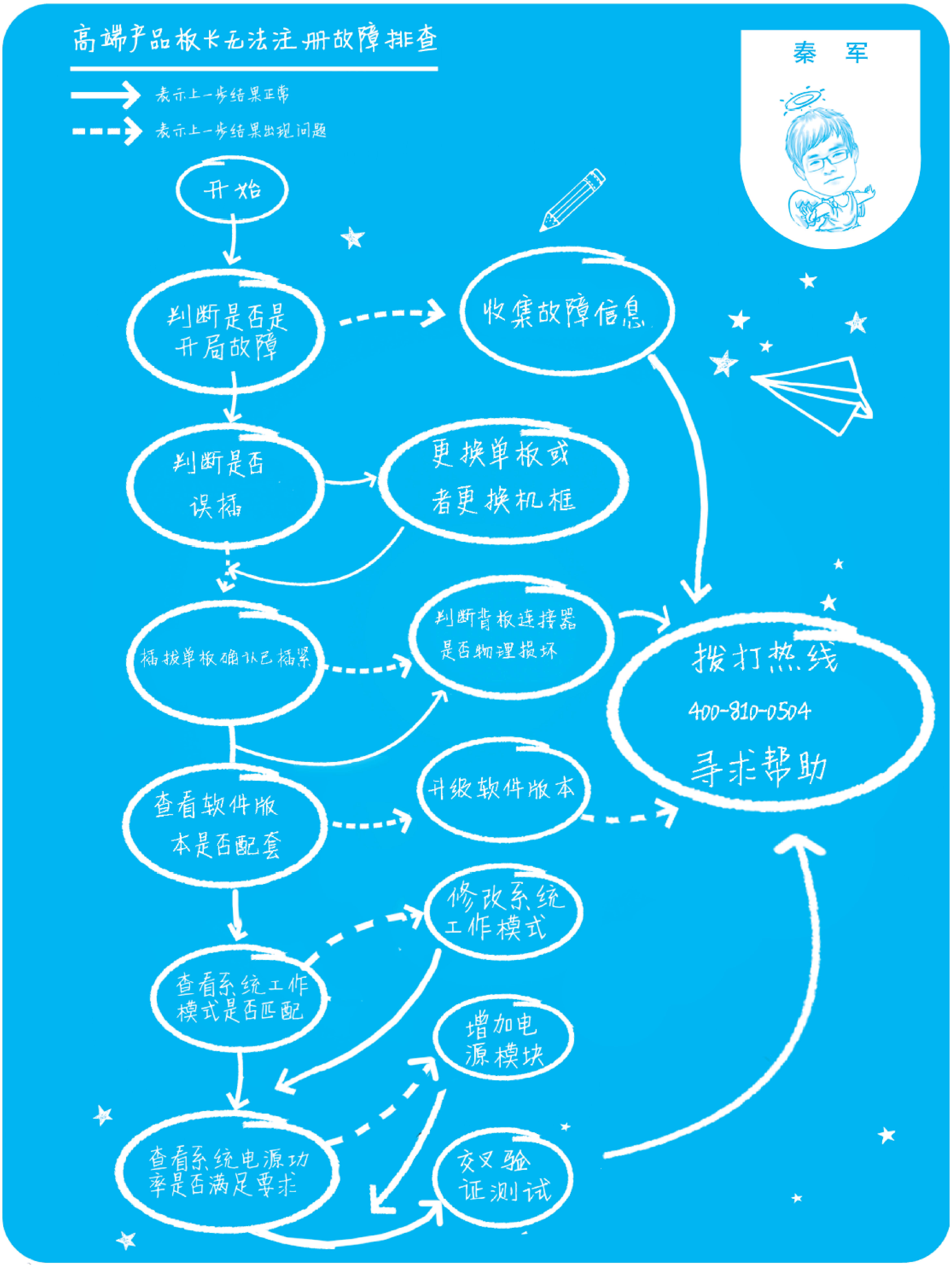
<H3C> display acl ipv6 inbound
```

```
Current ACL IPv6 inbound mode                : Disable
ACL IPv6 inbound mode after system restart: Disable
Notice: Changing ACL IPv6 mode will take effect only after system restart.

<H3C> display acl mode
Current ACL mode                : advanced
ACL mode after system restart: advanced
Notice: Changing ACL mode will take effect only after system restart.

[H3C]display this
acl ipv6 enable
 acl mode advanced
 portal-roaming enable
 undo vpn popgo
 system working mode routee
 irf mode enhanced
```

通过以上步骤仍然无法建立 IRF2，请拨打热线 400-810-0504 寻求帮助。


高端产品板卡无法注册故障排查
表示上一步结果正常
表示上一步结果出现问题
秦 军
开始
判断是否是开局故障
收集故障信息
判断是否误插
更换单板或者更换机框
插拔单板确认已插紧
判断背板连接器是否物理损坏
拨打热线
400-810-0504
寻求帮助
查看软件版本是否配套
升级软件版本
修改系统工作模式
查看系统工作模式是否匹配
增加电源模块
查看系统电源功率是否满足要求
交叉验证测试

1. 开始

单板无法注册时应首先进行如下排查后方可怀疑是硬件故障。

2. 流程图相关操作说明

(1) 判断是否是开局故障

如果是开局故障,请继续按照如下方法排查;如果是设备使用中出现的故障,请直接收集故障信息并联系 400。

(2) 插拔单板确认已插紧

① 拔出单板后,首先判断单板后部与背板相连的连接器是否故障,是否受到物理损坏;如果是,请直接联系 400 更换单板解决;如果不是,则继续按照以下方法排查。

② 安装单板时,将单板前面板两侧的扳手往外旋转,然后一只手托住单板(注意不要碰到电路板上的元件),另一只手握住单板前面板,沿着插槽导轨平稳插入。

③ 将扳手向内合拢,使单板与背板紧密接触。

④ 手动将螺钉导正后拧入,再用螺丝刀拧紧单板上的松不脱螺钉,固定单板。

如图 5-1 所示是 S12504 单板安装操作举例。

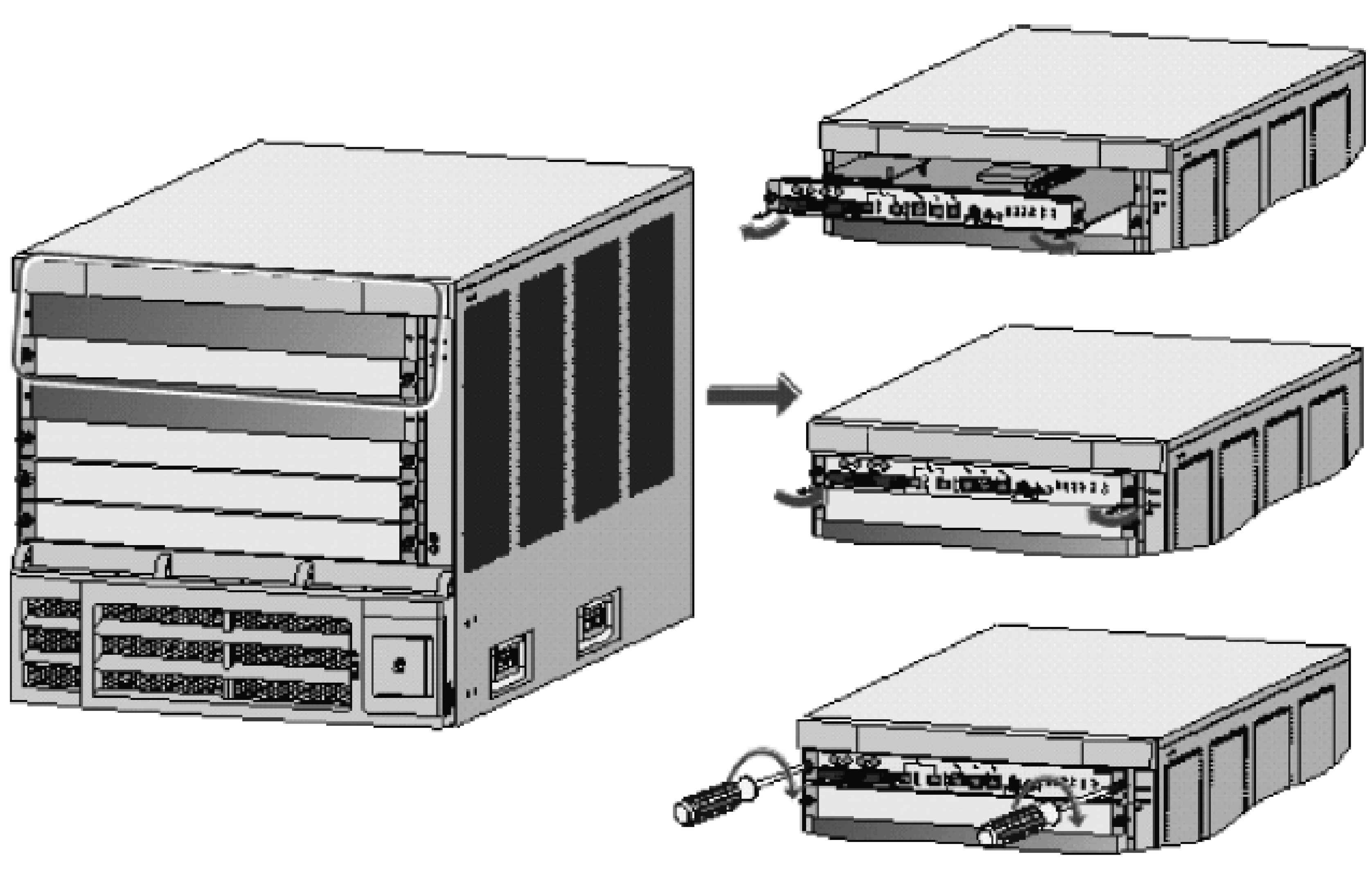


图 5-1　S12504 单板安装操作

(3) 查看软件版本是否配套

确认软件版本与单板的配套关系,排除软件版本过低导致新发货单板无法注册;请查看对应版本的版本说明书。

请查看版本说明书中的版本硬件特性,表 5-3 是 S12500 R1828P01 版本说明书的版本硬件特性列表举例。

表 5-3　S12500 R1828P01 版本硬件特性列表

项　　目	描　　述
可选单板类型	主控板: H3C S12500 管理及路由处理板,LST1MRPNC1

续表

项　目	描　述
可选单板类型	以太网接口板： 8 端口万兆以太网光接口业务板(LEB),(SFP+,LC)LST2XP8LEB1 8 端口万兆以太网光接口业务板(LEC),(SFP+,LC)LST2XP8LEC1 8 端口万兆以太网光接口业务板(LEF),(SFP+,LC)LST2XP8LEF1 32 端口万兆以太网光接口业务板(REB),(SFP+,LC)LST2XP32REB1 32 端口万兆以太网光接口业务板(REC),(SFP+,LC)LST2XP32REC1 48 端口千兆以太网电接口业务板(LEB)-(RJ45),LST1GT48LEB1 48 端口千兆以太网电接口业务板(LEC)-(RJ45),LST1GT48LEC1 48 端口千兆以太网光接口业务板(LEB)-(SFP,LC),LST1GP48LEB1 48 端口千兆以太网光接口业务板(LEC)-(SFP,LC),LST1GP48LEC1 4 端口万兆以太网光接口业务板(LEB)-(XFP,LC),LST1XP4LEB1 4 端口万兆以太网光接口业务板(LEC)-(XFP,LC),LST1XP4LEC1 8 端口万兆以太网光接口业务板(LEB)-(XFP,LC),LST1XP8LEB1 8 端口万兆以太网光接口业务板(LEC)-(XFP,LC),LST1XP8LEC1 32 端口万兆以太网光接口业务板(REB)-(SFP+,LC),LST1XP32REB1 32 端口万兆以太网光接口业务板(REC)-(SFP+,LC),LST1XP32REC1 48 端口千兆以太网光接口业务板(LEF)-(SFP,LC),LST1GP48LEF1 8 端口万兆以太网光接口业务板(LEF)-(XFP,LC),LST1XP8LEF1 8 端口万兆以太网光接口业务板(LEB)-(XFP,LC),LST3XP8LEB1 8 端口万兆以太网光接口业务板(LEC)-(XFP,LC),LST3XP8LEC1 16 端口万兆以太网光接口业务板(LEB)-(SFP+,LC),LST1XP16LEB1 16 端口万兆以太网光接口业务板(LEC)-(SFP+,LC),LST1XP16LEC1 8 端口万兆以太网光接口业务板(LEC)-(SFP+,LC),LST2XP8LEC2 16 端口万兆以太网光接口业务板(LEC)-(SFP+,LC),LST1XP16LEC2 32 端口万兆以太网光接口业务板(REC)-(SFP+,LC),LST2XP32REC2 48 端口千兆以太网光接口业务板(LEC)-(SFP,LC),LST1GP48LEC2 48 端口千兆以太网电接口业务板(LEC)-(RJ45),LST1GT48LEC2 OAA 单板： H3C S12500,防火墙业务板,LST1FW2A1,LST1FW3A1 H3C S12500,入侵防御系统模块,LST1IPS1A1,LST1IPS2A1 H3C S12500,NetStream 业务板,LST1NSM1A1 H3C S12500,负载均衡业务板,LST1LB1A1 H3C S12500,应用控制网关业务板模块,LST1ACG1A1 交换网板： H3C S12518 交换网板,LST1SF18B1 H3C S12508 交换网板,LST1SF08B1 H3C S12518 交换网板,LST1SF18C1 H3C S12518 交换网板,LST2SF18C1 H3C S12508 交换网板,LST2SF08C1

(4) 查看系统工作模式是否匹配

请查看相关产品的操作手册，在“基础配置→设备管理→配置系统工作模式”这一节中，对于不同的系统工作模式支持的单板类型有详细说明。

命令：*display system working mode*

例如：通过命令查看，可以确认 SR8800 的系统工作模式为 hybrid。

```
<H3C>display system working mode
Current system working mode       : hybrid
Working mode after system restart: hybrid
Notice: Changing working mode will take effect only after system restart.
```

（5）查看系统电源功耗是否满足要求

请查看相关产品安装指导，查询并计算设备的电源模块输出功率，查询设备的单板、风扇的功耗，并计算设备总功耗，确认系统电源输出功率足够满足新单板上电需求。如果不能满足，则需要增加电源模块。

（6）对于备用主控板要检查备用主控板版本是否与主用主控板一致

请查看对应版本的版本说明书，按照版本说明书的指导，在 bootware 菜单下同步备用主控板版本。

（7）交叉验证测试

将无法注册成功的单板 A 和能够注册成功的单板 B 互换槽位测试。

如果单板 A 在新的槽位上依然无法注册成功，同时单板 B 能够注册成功，则可以初步怀疑是单板自身故障导致无法注册成功；如果单板 A 在新的槽位上可以注册成功，同时单板 B 无法注册成功，则可以初步怀疑是主控板或者机框故障导致单板无法注册成功。

S12500/S9500E产品风扇故障排查





1. 开始

S12500/S9500E 产品出现风扇故障问题，首先应确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

如果风扇指示灯异常，或者命令行查询到风扇运行状态异常，或者设备打印风扇异常信息，则需要拔出风扇框观察确认是否有风扇停转，插拔风扇框并交叉验证确认故障，是否有异物。确认故障后需要收集相关故障信息反馈 400。

如果风扇指示灯正常，命令行查询风扇运行状态正常，同时设备没有打印风扇异常信息，则说明风扇运行正常，如果还有疑问，请拨打 400-810-0504 寻求帮助。

2. 流程图相关操作说明

(1) 确认故障现象

确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

① 风扇框指示灯说明。风扇框指示灯说明如表 5-4 所示。

表 5-4 风扇框指示灯说明

指示灯	颜色	状态	含 义
RUN	绿色	灯灭	风扇框出现故障
		灯闪烁	风扇框处于正常运行状态
ALM	红色	灯灭	风扇框处于正常运行状态
		灯闪烁	风扇框处于故障状态
		灯常亮	

② 命令行确认风扇运行状态，Normal 表示状态正常，Fault 和 Absent 表示状态异常，或者风扇框不在位。

```
<H3C>display fan
Fan-tray state on chassis 0:
Fan-tray   1    state: Normal
```

③ 设备打印风扇异常信息如下。

```
%Jun 26 10:12:24:805 2013 H3C DEV/3/FAN_ABSENT:Chassis 2 Fan 1 is absent. %Jun 26 10:12:32:805 2013 H3C DEVD/2/DRV_DEV_FAN_CHANGE: Chassis 2: Fan communication state changed: Fan 1 changed to fault. %Jun 26 10:12:42:405 2013 H3C DEV/2/FAN_FAILED:Chassis 2 Fan 1 failed.
```

(2) 判断风扇是否停转，是否有异物

① 拔出风扇框，(正常情况下，由于惯性的力量，风扇框在刚拔出来的时候，风扇的扇叶还是会继续旋转一段时间，如果有风扇没有在旋转状态，则说明该风扇之前已处于停止转动的异常状态)观察是否有风扇处于停止状态，如果有，则可以判断风扇故障，如果没有，请继续按照后续步骤排查。

② 拔出风扇框后，查看风扇框内是否有异物，如果有异物，会导致风扇运行异常，清除异物解决；如果确认没有异物，请继续按照后续步骤排查。

(3) 插入风扇框确认插紧

风扇框没有插紧，会导致风扇运行状态异常。

① 插入风扇框，抬起风扇框插入机框风扇框槽位，向内缓慢推入到底；手动将风扇框面板两侧的松不脱螺钉导正后拧入，再使用螺丝刀拧紧螺钉，以确保良好固定。

② 观察风扇是否正常运行，指示灯状态是否正常，命令行查询风扇运行状态是否正常，是否有风扇异常信息打印；如果风扇运行恢复正常，则说明之前风扇框没有插紧；如果故障现象仍存在，请继续按照后续步骤排查。

(4) 交叉验证

交叉验证，即把疑似故障的风扇框和正常运行的风扇框互换机框测试，确认故障是跟着风扇框走，还是跟着机框走；如果故障跟着风扇框走，则为风扇框故障，请更换解决，否则为机框故障，请按照后续步骤收集信息并将排查结果反馈400。如果现场不存在交叉验证的条件，请按照后续步骤收集信息并反馈400。

以上所有操作请在征得客户同意下进行，根据交叉验证的结果确认故障所在，拨打400-810-0504寻求帮助。

(5) 收集故障信息

确认电源状态异常，或者日志中有电源异常告警信息，需要收集故障信息，反馈给400排查。

故障信息请收集设备的诊断信息、日志信息文件和diagfile文件，具体收集方法如下。

① 收集设备诊断信息。

命令：*display diagnostic-information*

执行完上述这条命令之后，请将在CF卡根目录中生成的diag文件导出来保存。

例如：

```
<H3C>display diagnostic-information
-----------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( * .diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

   0    drw-          -   Jul 07 2013 07:16:12   logfile
   1    drw-          -   Jul 07 2013 07:13:04   diagfile
   2    -rw-    4924407   May 06 2013 06:43:32   default.diag
   3    drw-          -   May 02 2013 03:31:52   diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

② 收集设备日志信息文件。

命令：*logfile save*

执行完上述命令后，将CF卡的logfile文件夹中的logfile文件全部导出来保存。

例如：

```
<H3C>logfile save
----------------------------------------------------------------------
Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

  0     -rw-   10484413   Dec 26 2013 08:37:00    logfile1.log
  1     -rw-     150941   Dec 14 2013 10:10:54    logfile.log
  2     -rw-     127193   Jan 21 2013 09:41:28    logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

③ 收集设备 diagfile 信息文件。

(S9500/S8500、SR8800 的 R32XX 版本及之前版本，没有该文件，无须收集。)

在系统视图下输入_hide，进入到隐含模式。

命令：*_diagnose-file save*

执行完上述命令后，将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如：

```
[H3C]_hide
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]_diagnose-file save
----------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

   0     -rw-    2418760   Jul 09 2013 01:43:16    diagfile1.log
   1     -rw-      69266   Dec 03 2013 09:38:36    diagfile.log
   2     -rw-    4291181   Dec 10 2013 12:27:48    diagfile2.log
   3     -rw-     292979   Jul 07 2013 07:31:52    diagfile3.log
   4     -rw-    5240510   Jul 08 2013 11:55:00    diagfile4.log
   5     -rw-     110346   Jul 07 2013 08:51:44    diagfile5.log
   6     -rw-     192711   Jul 09 2013 12:03:26    diagfile6.log
   7     -rw-     166363   Jul 09 2013 08:38:20    diagfile7.log
   8     -rw-      17121   Jul 08 2013 16:37:48    diagfile8.log
   9     -rw-     101888   Jul 07 2013 07:54:28    diagfile9.log
   10    -rw-    2375568   Jul 09 2013 08:06:34    diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```

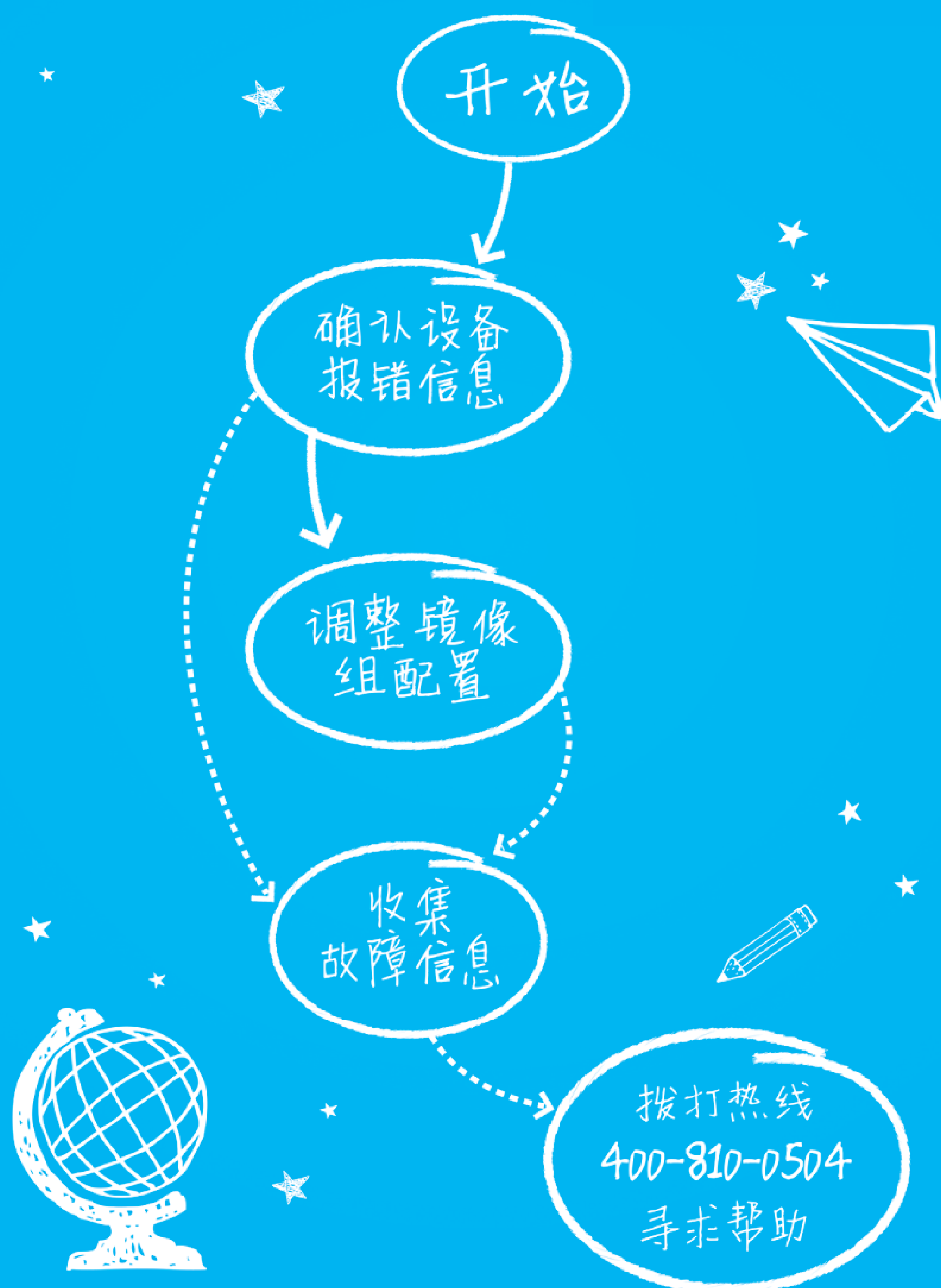
张 磊



S12500/S9500E产品镜像组无法下发故障排查

→ 表示上一步结果正常

⇢ 表示上一步结果出现问题



1．开始

S12500/S9500E 产品出现镜像组无法下发问题，首先应该确认设备报错信息，然后根据报错信息原因判断镜像组无法下发的原因，并采用相应解决方法。

如果设备没有报错信息，请收集信息并拨打 400-810-0504 寻求帮助。

2．流程图相关操作说明

（1）确认设备报错信息

镜像组下发时，如果镜像组配置超过了设备自身的硬件规格，设备会提示错误，此时需要调整镜像组配置解决。

请确认设备报错信息是否是如下报错信息中的一种，如果不是或者没有报错，请按照后续步骤收集信息，并拨打 400-810-0504 寻求帮助。

```
Error: Local mirroring-group number exceeds hardware capability.
Error: Failed to configure port mirroring due to hardware unsupported!
```

以上报错可能会在命令行下发镜像组配置时出现。

（2）调整镜像组配置

①“Error: Local mirroring-group number exceeds hardware capability.”。

打印上述告警的原因为镜像组配置遇到如下设备限制。

（a）S9500E/S12500 不支持一对多的镜像，即将一个端口的报文镜像到多个监控端口上。

（b）S9500E/S12500 只支持入方向流镜像。

（c）同一个端口不可以作为不同镜像组的监控端口和被监控端口。

（d）S9500E 的端口镜像支持同方向（分为入方向和出方向）的分析口数量存在下面的限制。

对于 24 个端口的 GE 接口线卡板，1 块单板只支持配置 1 个分析口。

对于 48 个端口的 GE 接口线卡板（除了 LSR2GV48REB1 单板之外），1 个单板支持配置 2 个分析口，其中前 24 个端口支持配置 1 个分析口，后 24 个端口支持配置 1 个分析口。

对于 LSR2GV48REB1 单板，1 块单板只支持配置 1 个分析口。

对于 10GE 接口线卡板（除了 LSR1XP16REB1 单板之外），按照端口顺序，单板上每 2 个 10GE 端只支持配置 1 个分析口。

对于 LSR1XP16REB1 单板，1 个单板支持配置 2 个分析口，按照端口顺序，前 8 个 10GE 端口支持配置 1 个分析口，后 8 个 10GE 端口支持配置 1 个分析口。

（e）S12500 的端口镜像支持同方向（分为入方向和出方向）的分析口数量存在下面的限制。

对于 24 个端口的 GE 接口线卡板，1 块单板只支持配置 1 个分析口。

对于 48 个端口的 GE 接口线卡板，1 块单板支持配置 2 个分析口，其中前 24 个端口支持配置 1 个分析口，后 24 个端口支持配置 1 个分析口。

对于 10GE 接口线卡板（除了 LST1XP32R 单板之外），按照端口顺序，单板上每 2 个 10GE 端口只支持配置 1 个分析口。

对于 LST1XP32R 单板，1 个单板支持配置 4 个分析口，按照端口顺序，前 8 个 10GE 端口支持配置 1 个分析口，后 8 个 10GE 端口支持配置 1 个分析口。

请调整镜像组端口，以规避上述设备限制。

如果要实现一对多镜像，具体规避解决方法请参考《百日维新》第一期案例“一法定乾坤——S12500S9500E 交换机镜像功能限制问题的解决方法”，和 DMP 归档案例“高端产品镜像限制与解决方法总结 V1.0 耿古月”（归档路径：技术支持中心- S12500/S9500E-6 经验案例）。

② “Error: Failed to configure port mirroring due to hardware unsupported!”。

IRF 模式下，设备不支持跨框配置端口镜像。如果配置镜像的目的端口和源端口位于 IRF 模式下的两台不同的设备上，就会打印上述提示信息。

规避方法请参考《百日维新》第一期案例“一法定乾坤——S12500S9500E 交换机镜像功能限制问题的解决方法”，和 DMP 归档案例“高端产品镜像限制与解决方法总结 V1.0 耿古月”（归档路径：技术支持中心- S12500/S9500E-6 经验案例）。

如果排除以上问题后，单板 CPU 利用率还存在异常高的问题，请拨打 400-810-0504 寻求帮助。

(3) 收集故障信息

确认电源状态异常，或者日志中有电源异常告警信息，需要收集故障信息，反馈给 400 排查。

故障信息请收集设备的诊断信息、日志信息文件和 diagfile 文件，具体收集方法如下。

① 收集设备诊断信息。

命令：*display diagnostic-information*

执行完上述这条命令之后，请将在 CF 卡根目录中生成的 diag 文件导出来保存。

例如：

```
<H3C>display diagnostic-information
------------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name( * .diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
Directory of cfa0:/

   0     drw-          -   Jul 07 2013 07:16:12   logfile
   1     drw-          -   Jul 07 2013 07:13:04   diagfile
   2     -rw-    4924407   May 06 2013 06:43:32   default.diag
   3     drw-          -   May 02 2013 03:31:52   diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

② 收集设备日志信息文件。

命令：*logfile save*

执行完上述命令后，将 CF 卡的 logfile 文件夹中的 logfile 文件全部导出来保存。

例如：

```
<H3C>logfile save
--------------------------------------------------------------------------
 Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

   0     -rw-   10484413   Dec 26 2013 08:37:00    logfile1.log
   1     -rw-     150941   Dec 14 2013 10:10:54    logfile.log
   2     -rw-     127193   Jan 21 2013 09:41:28    logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

③ 收集设备 diagfile 信息文件。

(S9500/S8500、SR8800 的 R32XX 版本及之前版本,没有该文件,无须收集。)

在系统视图下输入_hide,进入到隐含模式。

命令:*_diagnose-file save*

执行完上述命令后,将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如:

```
[H3C]_hide
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]_diagnose-file save
--------------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

   0     -rw-    2418760   Jul 09 2013 01:43:16    diagfile1.log
   1     -rw-      69266   Dec 03 2013 09:38:36    diagfile.log
   2     -rw-    4291181   Dec 10 2013 12:27:48    diagfile2.log
   3     -rw-     292979   Jul 07 2013 07:31:52    diagfile3.log
   4     -rw-    5240510   Jul 08 2013 11:55:00    diagfile4.log
   5     -rw-     110346   Jul 07 2013 08:51:44    diagfile5.log
   6     -rw-     192711   Jul 09 2013 12:03:26    diagfile6.log
   7     -rw-     166363   Jul 09 2013 08:38:20    diagfile7.log
   8     -rw-      17121   Jul 08 2013 16:37:48    diagfile8.log
   9     -rw-     101888   Jul 07 2013 07:54:28    diagfile9.log
   10    -rw-    2375568   Jul 09 2013 08:06:34    diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```

高端交换机策略路由不生效故障排查

赵 跃



1. 开始

策略路由不生效问题定位故障的思路是：先查看 ACL 规则是否匹配了流量，ACL 资源是否超规格，之后查看策略路由下一跳是否可达，最后查看是否配置了 packet-filter/QoS 策略等功能与策略路由冲突。

2. 流程图相关操作说明

(1) 查看 ACL 规则是否匹配流量

查看 ACL 规则的配置，确认 ACL 规则匹配了流量。

命令：*display acl acl-number*

例如：通过命令确认 ACL 规则是否匹配了需要做策略路由的流量。

```
<H3C>display acl 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 permit ip source 10.0.0.0 0.0.0.255
 rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 100.0.0.0 0.0.0.255
```

(2) 修改/增加 ACL 规则

若通过 display acl 命令，查看规则中所写的 rule 规格错误，则需要重新下发 rule 命令，修改 rule 规则，确保 rule 规则匹配到流量。如果 ACL 中 rule 规则没有匹配所需做策略路由的流量，则需新增 rule 规则匹配该流量。

命令：*rule*

例如：ACL 规则中将需要做策略路由的源 IP 为 20.0.0.0/24、目的 IP 为 200.0.0.0/24 的流量错误写为源 IP 为 20.0.0.0/24、目的 IP 为 100.0.0.0/24，同时漏写源 IP 为 30.0.0.0/24 的流量，则需下发命令更正和增加 ACL 规则。

```
[H3C-acl-adv-3000]rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 200.0.0.0 0.0.0.255
Info: The rule id already exists, and the current operation is modifying the rule.
[H3C-acl-adv-3000]rule 10 permit ip source 30.0.0.0 0.0.0.255
[H3C-acl-adv-3000]display this
#
acl number 3000
 rule 0 permit ip source 10.0.0.0 0.0.0.255
 rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 200.0.0.0 0.0.0.255
 rule 10 permit ip source 30.0.0.0 0.0.0.255
```

(3) 检查 ACL 资源是否超规格

查看单板 ACL 资源利用情况，判断 ACL 资源是否已被耗尽，导致下发的 ACL 规则实际没有生效。

V5 平台命令：*display acl resource*

V7 平台命令：*dis qos-acl resource slot number*

例如：通过下发命令查看，各个槽位单板 ACL 资源利用情况。

① V5。

```
<H3C>display acl resource
Interface:
GE2/0/1 to GE2/0/24
--------------------------------------------------------------------------
 Type          Total     Reserved    Configured   Remaining    Usage
--------------------------------------------------------------------------
ACL rule       2048      0           1978         70           96%
Inbound ACL    2048      0           1978         70           96%
 OutboundACL   2048      0           0            70           0%

Interface:
   XGE3/0/1 to XGE3/0/2
--------------------------------------------------------------------------
 Type          Total     Reserved    Configured   Remaining    Usage
--------------------------------------------------------------------------
 ACL rule      8192      96          3            8093         1%
 Inbound ACL   8192      96          3            8093         1%
 OutboundACL   8192      0           0            8093         0%

 Interface:
   XGE3/0/3 to XGE3/0/4
--------------------------------------------------------------------------
 Type          Total     Reserved    Configured   Remaining    Usage
--------------------------------------------------------------------------
 ACL rule      8192      96          3            8093         1%
 Inbound ACL   8192      96          3            8093         1%
 OutboundACL   8192      0           0            8093         0%
```

② V7。

```
[H3C]dis qos-acl resource   slot  2
Interfaces: GE2/0/1 to GE2/0/24
-----------------------------------------------------------------------------
 Type              Total     Reserved    Configured   Remaining   Usage
-----------------------------------------------------------------------------
 ACL rule          8192      96          6            8090        1%
 Inbound ACL       8192      96          5            8090        1%
 Outbound ACL      8192      0           1            8090        0%
 IN-MQC-CAR        8192      0           0            8192        0%
 IN-COMM-CAR       7168      0           0            7168        0%
 IN-COUNT          8192      0           64           8128        0%
 OUT-MQC-CAR       8192      0           64           8128        0%
 OUT-COUNT         8192      0           64           8128        0%
```

ACL 资源是按芯片划分的，并且 Inbound/Outbound 方向共用芯片 ACL 资源。通过 display acl resource 命令可以看到所有槽位芯片 ACL 资源的利用情况，如上 V5 所示，2 槽位单板的 GE2/0/1 至 GE2/0/24 属于同一个芯片，2048 的 ACL 资源由这 24 个接口共用。从示例中看到 2 槽位单板 2048 的 ACL 资源已利用了 96%，已接近 ACL 资源耗尽，会导致涉及 ACL 下发的功能正常应用，包括策略路由的使用。而 3 槽位的 XG3/0/1 和 XG3/0/2 属于同一个芯片，共用 8192 的 ACL 资源，当前 ACL 资源利用率为 1%，ACL 资源充足。XG3/0/3

和 XG3/0/4 类似。V7 平台的情况一样。

（4）检查策略路由下一跳是否可达

检查策略路由配置中下一跳是否可达，如查看接口状态、ARP 表项、路由表或 ping 测试。

命令：*display interface interface-type interface-number*

displayarp x.x.x.x

display ip routing-table x.x.x.x

ping x.x.x.x

例如：策略路由下一跳配置为 100.0.0.2，通过查看接口状态、ARP 表项、路由表或 ping 测试确定策略路由下一跳是否可达。

```
<H3C>display  interface GigabitEthernet 2/0/1
 GigabitEthernet2/0/1 current state:Up
…

<H3C>displayarp 100.0.0.2
                Type: S-Static    D-Dynamic    A-Authorized    M-Multiport
IP Address       MAC Address      VLANID  Interface          Aging Type
100.0.0.2        0023-8911-7d00   100     GE2/0/1             N/A   D

<H3C>displayip routing-table 100.0.0.2
RoutingTable : Public
SummaryCount : 1

Destination/Mask        Proto  Pre  Cost        NextHop         Interface

100.0.0.0/24            Direct  0    0          100.0.0.1       Vlan100

<H3C>ping 100.0.0.2
  PING 100.0.0.2:56  data bytes, press CTRL_C to break
    Reply from 100.0.0.2: bytes=56 Sequence=0ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=1ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=2ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=3ttl=255 time=2 ms
    Reply from 100.0.0.2: bytes=56 Sequence=4ttl=255 time=1 ms

  --- 100.0.0.2ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

（5）排查路由

策略路由下一跳不通，需要排查路由问题。

（6）检查设备是否配置了 packet-filter/QoS 策略等功能

当设备在相关视图下配置了 packet-filter 或 QoS 策略功能，由于 packet-filter 和 QoS 策略的优先级比策略路由高，因而策略路由下发不生效。需要结合所需做策略路由的流量 ACL 规则，对配置进行排查。

命令：*display qos policy interface interface-type interface-number*

display packet-filter

例如：acl number 3000 匹配了所需做策略路由的流量，同时在设备上下发了 packet-filter/QoS 策略功能。packet-filter 可以在二/三层物理接口及三层虚接口上下发，设备上可以配置基于接口/VLAN/全局/控制平面应用的 QoS 策略，均需要排查。需注意，如下示例中，acl number 3000 同时作为策略路由、packet-filter、QoS 策略的感兴趣流量匹配条件，并且实际现网中可能存在不同 ACL，但是规则匹配相同的流量做 packet-filter/QoS 策略，也会造成策略路由不生效，因此需要排查不同的 ACL 中是否有相同的 rule 规则。

说明：设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 之前的版本，策略路由的优先级低于 QoS 策略，涉及 QoS 策略功能部分的排查。而设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 及之后的版本，策略路由的优先级高于 QoS 策略，不涉及 QoS 策略功能部分的排查。

```
[H3C]dis packet-filter all
  Interface: Vlan-interface100
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
[H3C-Vlan-interface100]dis this
#
interface Vlan-interface100
 ip address 100.0.0.1 255.255.255.0
 packet-filter 3000 inbound
 ip policy-based-route 1
#
return

[H3C]display qos policy interface GigabitEthernet 2/0/1
  Interface: GigabitEthernet2/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: 1
      Accounting Enable:
        0 (Packets)
      Redirect enable:
      Redirect type: next-hop
      Redirect destination:
        200.0.0.2
      Redirect fail-action: forward
[H3C-GigabitEthernet2/0/1]dis this
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port access vlan 100
 qos apply policy 1 inbound
#
return
```

（7）修改配置

通过上一步的排查发现策略路由与 packet-filter/QoS 策略同时下发，导致策略路由不生

效，需修改配置。

① 策略路由与 packet-filter 同时下发的情况。包过滤下发在 Inbound 方向时，将导致策略路由感兴趣的流量在执行策略路由动作之前被过滤掉。包过滤下发在 Outbound 方向时，将导致策略路由动作执行完后，报文被过滤掉，流量仍无法按策略路由需求转发出去。在上述两种情况下，均需要在 packet-filter 的 ACL 规则中，将需要正常转发的流量 rule 规则去掉。

② 策略路由与 QoS 策略同时下发的情况。策略路由感兴趣的流量先由 QoS 策略匹配后处理了。该种情况下，需重新了解和细化需求，是否可以通过细化 QoS 策略 ACL 规则和策略路由 ACL 规则，使两个 ACL 规则不冲突，流量能区分出来按不同的功能执行动作。

说明： 设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 之前的版本，策略路由的优先级低于 QoS 策略，涉及 QoS 策略功能部分的排查。而设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 及之后的版本，策略路由的优先级高于 QoS 策略，不涉及 QoS 策略功能部分的排查。


CR16000/SR8800产品风扇故障排查
张 磊
表示上一步结果正常
表示上一步结果出现问题
开始
确认故障现象
更换风扇框或者清除异物
判断风扇是否停转，是否有异物
插入风扇框确认插紧
交叉验证测试
收集故障信息
拨打热线
400-810-0504
寻求帮助

1. CR16000/SR8800 产品风扇故障排查

CR16000/SR8800 产品出现风扇故障问题，首先应确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

如果风扇指示灯异常，或者命令行查询到风扇运行状态异常，或者设备打印风扇异常信息，则需要拔出风扇框观察确认是否有风扇停转，插拔风扇框并交叉验证确认故障，是否有异物。确认故障后需要收集相关故障信息反馈 400。

如果风扇指示灯正常，命令行查询风扇运行状态正常，同时设备没有打印风扇异常信息，则说明风扇运行正常，如果还有疑问，请拨打 400-810-0504 寻求帮助。

2. 流程图相关操作说明

(1) 确认故障现象

确认风扇指示灯状态，命令行确认风扇运行状态、设备是否打印风扇异常信息。

① 风扇框指示灯说明。CR16000 风扇框指示灯说明如表 5-5 所示。

表 5-5 CR16000 风扇框指示灯说明

指示灯	颜色	状态	含　义
RUN	绿色	灯灭	风扇框出现故障
		灯闪烁	风扇框处于正常运行状态
ALM	红色	灯灭	风扇框处于正常状态
		灯闪烁	风扇框处于故障状态
		灯常亮	

SR8800 风扇框指示灯说明如表 5-6 所示。

表 5-6 SR8800 风扇框指示灯说明

指示灯	颜色	状态	含　义
RUN	绿色	灯灭	风扇框出现故障
		灯常亮	风扇框处于正常运行状态
ALM	红色	灯灭	风扇框处于正常状态
		灯常亮	风扇框处于故障状态

② 命令行确认风扇运行状态，Normal 表示状态正常，Fault 和 Absent 表示状态异常，或者风扇框不在位。

```
CR16000
<H3C>display fan
Fan-tray state on chassis 0:
Fan-tray  1     state: Normal
SR8800
<H3C>display fan
 Fan    1 State: Normal
```

③ 设备打印风扇异常信息。

```
%Jun 26 10:12:24:805 2013 H3C DEV/3/FAN_ABSENT:Fan 1 is absent.%Jun 26 10:12:32:805
2013 H3C DEVD/2/DRV_DEV_FAN_CHANGE: Fan communication state changed: Fan 1 changed to
fault.%Jun 26 10:12:42:405 2013 H3C DEV/2/FAN_FAILED:Fan 1 failed.
```

(2) 判断风扇是否停转,是否有异物

① 拔出风扇框,(正常情况下,由于惯性的力量,风扇框在刚拔出来的时候,风扇的扇叶还是会继续旋转一段时间,如果有风扇没有在旋转状态,则说明该风扇之前已处于停止转动的异常状态)观察是否有风扇处于停止状态,如果有,则可以判断风扇故障,如果没有,请继续按照后续步骤排查。

② 拔出风扇框后,查看风扇框内是否有异物,如果有异物,会导致风扇运行异常,清除异物解决;如果确认没有异物,请继续按照后续步骤排查。

(3) 插入风扇框确认插紧

风扇框没有插紧,会导致风扇运行状态异常。

① 插入风扇框,抬起风扇框插入机框风扇框槽位,向内缓慢推入到底;手动将风扇框面板两侧的松不脱螺钉导正后拧入,再使用螺丝刀拧紧螺钉,以确保良好固定。

② 观察风扇是否正常运行,指示灯状态是否正常,命令行查询风扇运行状态是否正常,是否有风扇异常信息;如果风扇运行恢复正常,则说明之前风扇框没有插紧;如果故障现象仍存在,请继续按照后续步骤排查。

(4) 交叉验证

交叉验证,即把疑似故障的风扇框和正常运行的风扇框互换机框测试,确认故障是跟着风扇框走,还是跟着机框走;如果故障跟着风扇框走,则为风扇框故障,请更换解决,否则为机框故障,请按照后续步骤收集信息并将排查结果反馈400。如果现场不存在交叉验证的条件,请按照后续步骤收集信息并反馈400。

以上所有操作请在征得客户同意下进行,根据交叉验证的结果确认故障所在,拨打400-810-0504寻求帮助。

(5) 收集故障信息

确认电源状态异常,或者日志中有电源异常告警信息,需要收集故障信息,反馈给400排查。

故障信息请收集设备的诊断信息、日志信息文件和diagfile文件,具体收集方法如下。

① 收集设备诊断信息。

命令:*display diagnostic-information*

执行完上述这条命令之后,请将在CF卡根目录中生成的diagfile文件导出来保存。

例如:

```
<H3C>display diagnostic-information
------------------------------------------------------------------------
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.
<H3C>dir cfa0:/
```

```
Directory of cfa0:/

   0    drw-           -  Jul 07 2013 07:16:12   logfile
   1    drw-           -  Jul 07 2013 07:13:04   diagfile
   2    -rw-     4924407  May 06 2013 06:43:32   default.diag
   3    drw-           -  May 02 2013 03:31:52   diaglog
1021088 KB total (554020 KB free)

File system type of cfa0: FAT32
```

② 收集设备日志信息文件。

命令：*logfile save*

执行完上述命令后，将 CF 卡的 logfile 文件夹中的 logfile 文件全部导出来保存。

例如：

```
<H3C>logfile save
------------------------------------------------------------------------
Saved the log file buffer to file cfa0:/logfile/logfile2.log successfully.
<H3C>dir cfa0:/logfile/
Directory of cfa0:/logfile/

   0    -rw-   10484413   Dec 26 2013 08:37:00    logfile1.log
   1    -rw-     150941   Dec 14 2013 10:10:54    logfile.log
   2    -rw-     127193   Jan 21 2013 09:41:28    logfile2.log

1021808 KB total (140128 KB free)

File system type of cfa0: FAT16
```

③ 收集设备 diagfile 信息文件。

（S9500/S8500、SR8800 的 R32XX 版本及之前版本，没有该文件，无须收集。）

在系统视图下输入_hide，进入到隐含模式。

命令：*_diagnose-file save*

执行完上述命令后，将 CF 卡的 diaglog 文件夹中的 log 文件全部导出来保存。

例如：

```
[H3C]_hide
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]_diagnose-file save
------------------------------------------------------------------------
Info: Diagnostic file buffer is empty.
[H3C-hidecmd]
<H3C>dir cfa0:/diaglog/
Directory of cfa0:/diaglog/

   0    -rw-    2418760   Jul 09 2013 01:43:16    diagfile1.log
   1    -rw-      69266   Dec 03 2013 09:38:36    diagfile.log
   2    -rw-    4291181   Dec 10 2013 12:27:48    diagfile2.log
   3    -rw-     292979   Jul 07 2013 07:31:52    diagfile3.log
```

```
    4     -rw-   5240510  Jul 08 2013 11:55:00   diagfile4.log
    5     -rw-    110346  Jul 07 2013 08:51:44   diagfile5.log
    6     -rw-    192711  Jul 09 2013 12:03:26   diagfile6.log
    7     -rw-    166363  Jul 09 2013 08:38:20   diagfile7.log
    8     -rw-     17121  Jul 08 2013 16:37:48   diagfile8.log
    9     -rw-    101888  Jul 07 2013 07:54:28   diagfile9.log
    10    -rw-   2375568  Jul 09 2013 08:06:34   diagfile10.log

127206 KB total (56252 KB free)

File system type of cfa0: FAT16
```


Smart Link故障排查
秦 军
表示上一步结果正常
表示上一步结果出现问题
开始
查看Smart Link组状态
查看MAC、ARP/ND表项学习是否正确
检查保护VLAN配置
检查接口配置
检查发送/接收控制VLAN
检查接口状态、链路状态
检查数据报文流量统计
检查Flush报文的收发信息
检查配置角色抢占
拨打热线
400-810-0504
寻求帮助

1. 开始

首先检查 Smart Link 组状态是否正常。如果 Smart Link 组正常，则检查相关设备的 MAC 和 ARP/ND 表项学习是否正确。若正确，则对数据报文进行流量统计，找到丢包的节点；若不正确，则检查 Smart Link 保护 VLAN、控制 VLAN 的配置，以及 Flush 报文的收发情况。如果 Smart Link 组不正常，则检查接口的配置、接口和链路状态以及角色抢占配置是否正确。

2. 流程图相关操作说明

(1) 查看 Smart Link 组状态

Smart Link 的端口状态分为 ACTIVE、STANDBY 和 Down，如果状态为 Down，则表明端口故障。检查 Smart Link 组中物理端口角色是否符合预期，状态是否异常。正常情况下，主端口处于 ACTIVE 状态，从端口处于 STANDBY 状态。

命令：*display smart-link group group-id*

例如：通过命令查看，可以确认 Smart Link 组中物理端口的角色和状态。

```
[H3C]display smart-link group 1
 Smart link group 1 information:
 Device ID: c4ca-d9c0-5138
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance    1
 Member                   Role      State       Flush-count  Last-flush-time
--------------------------------------------------------------------------------
 Ethernet2/0/1            MASTER  ACTIVE      3            01:55:27 2010/01/01
 Ethernet2/0/2            SLAVE   STANDBY     2            01:55:05 2010/01/01
```

(2) 检查接口配置

分别查看主/从端口的配置信息，确保加入了正确的 Smart Link 组。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看物理端口已加入 Smart Link 组，并且禁用了接口的 STP、RRPP 功能，并确保该端口不是聚合成员端口或业务环回组成员端口。

```
interface Ethernet2/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 port smart-link group 1 master
 #
interface Ethernet2/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
```

```
stp disable
 port smart-link group 1 slave
```

（3）检查接口状态、链路状态

检查主端口、从端口的状态，以及物理链路是否良好。

命令：*display interface interface-type interface-number*

例如：通过命令查看主端口状态是否Up，接口下是否有错包增长。

```
[H3C]display smart-link group 1
   …
 Ethernet2/0/1              MASTER    Down     3            01:55:27 2010/01/01
 Ethernet2/0/2              SLAVE     ACTIVE     4            22:08:51 2010/01/01
[H3C]display interface Ethernet 2/0/1
 Ethernet2/0/1 current state: Down
   …
Input: 35 input errors, 0 runts, 0 giants, 0 throttles
       35 CRC, 0 frame, - overruns, 0 aborts
       - ignored, - parity errors
   …
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

（4）检查配置角色抢占

当主链路故障，则从端口从STANDBY切换到ACTIVE，如果主链路恢复，默认情况下主端口不进行抢占，仍然保持阻塞状态。如果配置了主端口角色抢占，需要检查抢占延时是否过长。

命令：*display smart-link group group-id*

例如：通过命令查看，可以确认Smart Link组中物理端口的角色和状态。

```
[H3C]display smart-link group 1
 Smart link group 1 information:
 Device ID: c4ca-d9c0-5138
 Preemption mode: ROLE
 Preemption delay:1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance     1
 Member                    Role       State        Flush-count    Last-flush-time
-------------------------------------------------------------------------------------------
 Ethernet2/0/1             MASTER  ACTIVE      3              01:55:27 2010/01/01
 Ethernet2/0/2             SLAVE     STANDBY   2              01:55:05 2010/01/01
```

（5）查看MAC、ARP/ND表项学习是否正确

当发生链路切换，如果发生业务中断，则需要检查与成员端口相连设备的MAC、ARP/ND表项是否正确。

（6）检查数据报文流量统计

如果MAC、ARP/ND表项学习正确，但业务数据转发不通，则对业务报文做流量统计，查看报文在哪里被丢弃。

（7）检查保护 VLAN 配置

如果 MAC、ARP/ND 表项学习不正确，则检查是否正确配置了 MSTI 与保护 VLAN 的映射关系，并且在 Smart Link 组中调用。

命令：*display stp region-configuration*

display smart-link group group-id

例如：检查 MSTI 与保护 VLAN 的映射关系，并确定 MSTI 被正确的 Smart Link 组调用。

```
[H3C]display stp region-configuration
 Oper configuration
   Format selector          :0
   Region name              :000fe2f408d2
   Revision level           :0
   Configuration digest     :0x2cc089ef39bd9898636abaca225b26a9

   Instance    Vlans Mapped
      0          11 to 4094
      1          1    to 10
[H3C]display smart-link group 1
 Smart link group 1 information:
 Device ID: c4ca-d9c0-5138
 Preemption mode:ROLE
 Preemption delay:1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance      1
 Member                       Role       State        Flush-count    Last-flush-time
-------------------------------------------------------------------------------------
 Ethernet2/0/1                MASTER ACTIVE     3              01:55:27 2010/01/01
 Ethernet2/0/2                SLAVE    STANDBY  2              01:55:05 2010/01/01
```

（8）检查发送/接收控制 VLAN

在 Smart Link 设备上配置控制 VLAN，控制 VLAN 同时也是保护 VLAN，不同的 Smart Link 组需要配置不同的控制 VLAN。在相关设备上，从 Smart Link 设备到目的设备之间，主、从链路上的端口需要使能接收 Flush 报文功能，并且接收处理 Flush 报文的控制 VLAN 和在 Smart Link 设备上配置的发送控制 VLAN 要相同；同时，与 Smart Link 组成员端口相连的端口上关闭 STP。

命令：*display smart-link group group-id*

例如：在 Smart Link 设备上通过命令确认控制 VLAN 为 VLAN 10。

```
[H3C]display smart-link group 1
 Smart link group 1 information:
 Device ID: c4ca-d9c0-5138
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance      1
 Member                      Role       State        Flush-count Last-flush-time
-----------------------------------------------------------------------------------
 Ethernet2/0/1               MASTER  ACTIVE    3              01:55:27 2010/01/01
 Ethernet2/0/2               SLAVE    STANDBY  2              01:55:05 2010/01/01
```

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看与主/从端口相连的端口已关闭 STP，并使能了接收 Flush 报文功能，并且接收处理 Flush 报文的控制 VLAN 和与 Smart Link 设备上配置的发送控制 VLAN 相同。

```
interface Ethernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 10
 stp disable
 smart-link flush enable control-vlan 10
```

(9) 检查 Flush 报文的收发信息

当发生链路切换时，需要检查 Smart Link 设备是否发出了 Flush 报文以刷新 MAC、ARP/ND 表项，同时检查相关设备上是否收到了 Flush 报文。

命令：*display smart-link group group-id*

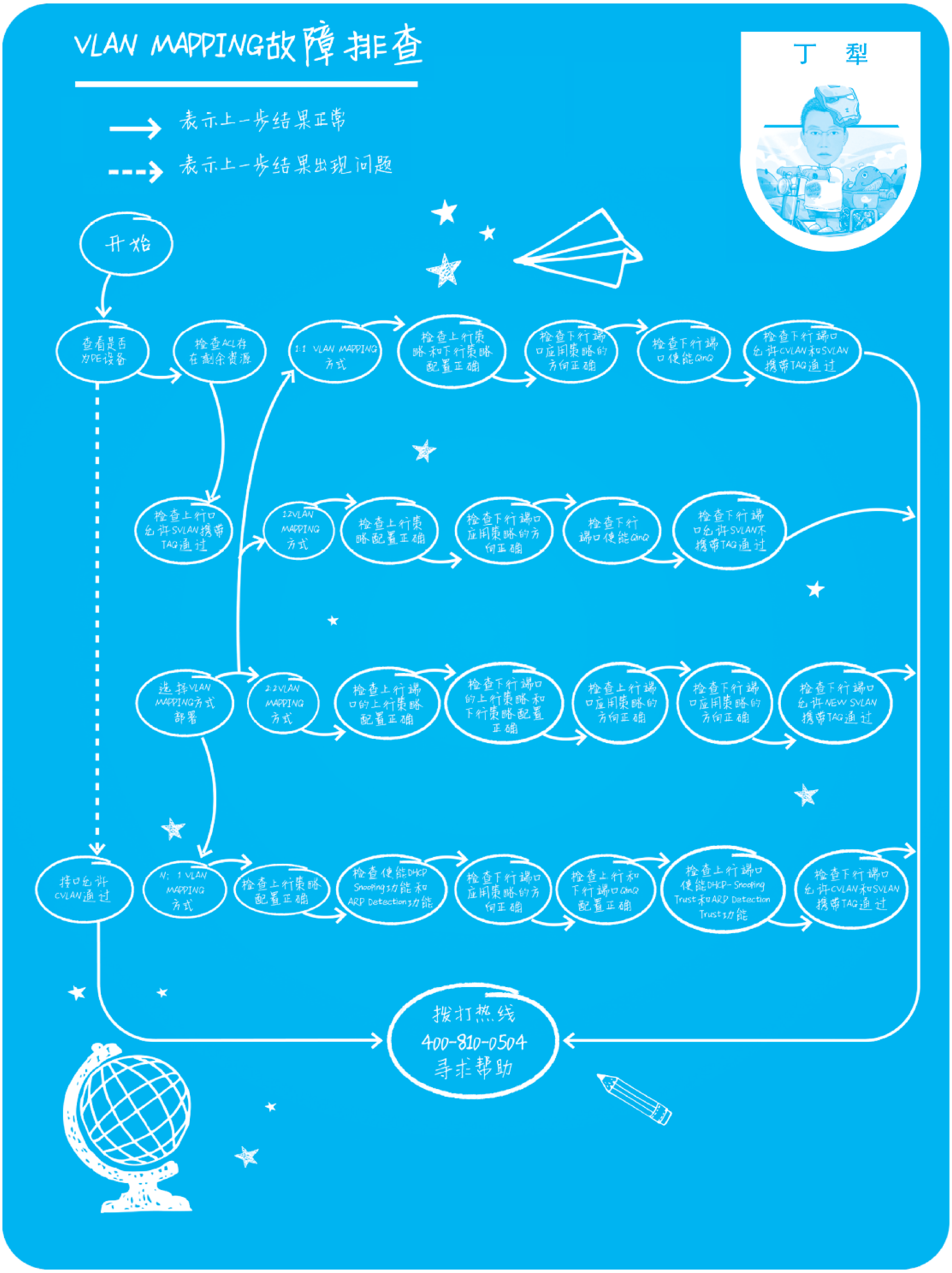
例如：在 Smart Link 设备上查看 Flush 报文的发送情况。

```
[H3C]display smart-link group 1
 Smart link group 1 information:
 Device ID:c4ca-d9c0-5138
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 10
 Protected VLAN: Reference Instance     1
 Member                    Role      State      Flush-count Last-flush-time
---------------------------------------------------------------------------
 Ethernet2/0/1             MASTER  ACTIVE    3            01:55:27 2010/01/01
 Ethernet2/0/2             SLAVE   STANDBY 2            01:55:05 2010/01/01
```

命令：*display smart-link flush*

例如：在相关设备上查看 Flush 报文的接收情况，包括接收到 Flush 报文的数量，最后一次接收 Flush 报文的端口、时间，以及 Flush 报文的 Device ID(与 Smart Link 组的 Device ID 相同)。

```
[H3C] display smart-link flush
 Received flush packets                          : 22
 Receiving interface of the last flush packet    :Ethernet1/0/2
 Receiving time of the last flush packet         :01:54:57 2010/01/01
 Device ID of the last flush packet              :c4ca-d9c0-5138
 Control VLAN of the last flush packet           : 10
```



VLAN MAPPING故障排查
丁 犁
表示上一步结果正常
表示上一步结果出现问题
开始
查看是否为PE设备
检查ACL存在剩余资源
1:1 VLAN MAPPING方式
检查上行策略和下行策略配置正确
检查下行端口应用策略的方向正确
检查下行端口使能QinQ
检查下行端口允许CVLAN和SVLAN携带TAG通过
检查上行口允许SVLAN携带TAG通过
1:2VLAN MAPPING方式
检查上行策略配置正确
检查下行端口应用策略的方向正确
检查下行端口使能QinQ
检查下行端口允许SVLAN不携带TAG通过
选择VLAN MAPPING方式部署
2:2VLAN MAPPING方式
检查上行端口的上行策略配置正确
检查下行端口的上行策略和下行策略配置正确
检查上行端口应用策略的方向正确
检查下行端口应用策略的方向正确
检查下行端口允许NEW SVLAN携带TAG通过
接口允许CVLAN通过
N: 1 VLAN MAPPING方式
检查上行策略配置正确
检查使能DHCP Snooping功能和ARP Detection功能
检查下行端口应用策略的方向正确
检查上行和下行端口QinQ配置正确
检查上行端口使能DHCP-Snooping Trust和ARP Detection Trust功能
检查下行端口允许CVLAN和SVLAN携带TAG通过
拨打热线
400-810-0504
寻求帮助

1. 开始

定位故障的思路是：如果是 PE 设备，首先检查设备 ACL 资源是否足够，再检查设备上行口是否允许正确的 SVLAN 携带 TAG 通过，最后根据部署的 VLAN MAPPING 进行相关部署的配置检查。

2. VLAN MAPPING 排错相关操作说明

CE 设备：检查 CE 设备端口允许 CVLAN 标签通过

命令：*display interface interface-type interface-number*

例如：通过命令查看，GE2/0/10 接口是否允许 CVLAN Tag 通过。

```
<H3C>display interface GigabitEthernet 2/0/10
…
PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 100, 200
  Trunk port encapsulation: IEEE 802.1q
…
```

PE 设备

(1) 检查 ACL 存在剩余资源

设备资源不足将导致 VLAN MAPPING 无法部署，请检查 ACL 资源是否剩余。

命令：*display acl resource*

例如：通过命令查看设备 ACL VFP 资源剩余 1535 条资源。

```
<H3C>display acl resource
 Interface:
   GE1/0/1 to GE1/0/24, XGE1/1/1 to XGE1/1/2
------------------------------------------------------------------------
 Type          Total      Reserved    Configured   Remaining   Usage
------------------------------------------------------------------------
 VFP ACL       2048       512         1            1535        25%
 IFP ACL       8192       2048        0            6144        25%
 IFP Meter     4096       1024        0            3072        25%
 IFP Counter   4096       1024        0            3072        25%
 EFP ACL       1024       0           0            1024        0%
 EFP Meter     512        0           0            512         0%
 EFP Counter   512        0           0            512         0%
```

(2) 检查上行口允许 SVLAN 携带 Tag 通过

命令：*display interface interface-type interface-number*

例如：通过命令查看，GE2/0/10 接口允许 SVLAN Tag 10 通过。注意，若部署 2:2 VLAN MAPPING 方式需要 NEW_SVLAN 携带 Tag 通过。

```
<H3C>display interface GigabitEthernet 2/0/10
…
PVID: 1
 Mdi type: auto
 Port link-type: trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 10, 200
  Trunk port encapsulation: IEEE 802.1q
…
```

(3) 选择 VLAN MAPPING 方式部署

根据现场部署的 VLAN MAPPING 方式,选择下列相关流量进行排查。

(4) 采用 1:1VLAN MAPPING 方式

若采用 1:1VLAN MAPPING 部署方式,请按照下列流量进行排查。

① 检查上行策略和下行策略配置正确。检查上行策略中 customer-vlan-id 为 CVLAN,Service VLAN ID 为 SVLAN。检查下行策略中 service-vlan-id 为 SVLAN,Customer VLAN ID 为 CVLAN。

命令:*display qos policy interface interface-type interface-number*

例如:通过命令查看,确认 PE 设备与 CE 互联 GE5/0/2 端口部署的上行策略 Customer-VLAN-ID 为 100,Service VLAN ID 为 10;部署的下行策略 Service-VLAN-ID 为 10,Customer-VLAN-ID 为 100。

```
<H3C>display qos policy interface GigabitEthernet 5/0/2

  Interface: GigabitEthernet5/0/2

  Direction: Inbound

  Policy: uplink_celue
   Classifier: uplink_celue
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
     Behavior: uplink_celue
      Marking:
        Remark Service VLAN ID 10

  Direction: Outbound

  Policy: downlink_celue
   Classifier: downlink_celue
     Operator: AND
     Rule(s) : If-match service-vlan-id 10
     Behavior: downlink_celue
      Marking:
        Remark Customer VLAN ID 100
```

② 检查下行端口应用策略的方向正确。检查下行端口 Remark-Service-VLAN-ID 部署在接口 Inbound 方向;Remark Customer VLAN ID 部署在接口 Outbound 方向。

命令:*display qos policy interface interface-type interface-number*

例如:通过命令查看,确认 PE 设备与 CE 互联 GE5/0/2 端口部署的 Remark Service

VLAN ID 策略在接口 Inbound 方向；部署的 Remark Customer VLAN ID 策略在接口 Outbound 方向。

```
<H3C>display qos policy interface GigabitEthernet 5/0/2

  Interface: GigabitEthernet5/0/2

  Direction: Inbound

  Policy: uplink_celue
   Classifier: uplink_celue
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
     Behavior: uplink_celue
      Marking:
        Remark Service VLAN ID 10

  Direction: Outbound

  Policy: downlink_celue
   Classifier: downlink_celue
     Operator: AND
     Rule(s) : If-match service-vlan-id 10
     Behavior: downlink_celue
      Marking:
        Remark Customer VLAN ID 100
```

③ 检查下行端口使能 QinQ。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看，确认在设备 GE5/0/2 端口使能 QinQ。

```
<H3C>display current-configuration interface GigabitEthernet 5/0/2
#
interface GigabitEthernet5/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 100
 qinq enable
 qos apply policy uplink_celue inbound
 qos apply policy downlink_celue outbound
#
```

④ 检查下行端口允许 CVLAN 和 SVLAN 携带 Tag 通过。

命令：*display interface*

例如：通过命令查看，确认设备 GE5/0/2 端口允许 CVLAN 100 和 SVLAN 10 报文带 Tag 通过。

```
<H3C>display interface GigabitEthernet 5/0/2
...
Link delay is 0(sec)
```

```
Port link-type: trunk
  VLAN passing   : 1(default vlan), 10
  VLAN permitted: 1(default vlan),10, 100
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
...
#
```

(5) 采用1:2 VLAN MAPPING方式

若采用1:2 VLAN MAPPING部署方式,请按照下列流量进行排查。

① 检查上行策略配置正确。检查上行策略中Customer-VLAN-ID为CVLAN,Top-Most VLAN-ID为SVLAN。

命令: *display qos policy interface interface-type interface-number*

例如:通过命令查看,确认PE设备与CE互联GE5/0/3端口部署的上行策略Customer-VLAN-ID为100,Top-Most VLAN-ID为10。

```
<H3C>display qos policy interface GigabitEthernet 5/0/3

  Interface: GigabitEthernet5/0/3

  Direction: Inbound

  Policy: uplink_1:2
   Classifier: uplink_1:2
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
     Behavior: uplink_1:2
      Nesting:
        Nest top-most vlan-id 10
```

② 检查下行端口应用策略的方向正确。检查下行端口Top-Most VLAN-ID策略部署在接口Inbound方向。

命令: *display qos policy interface interface-type interface-number*

例如:通过命令查看,确认PE设备与CE互联GE5/0/3端口部署的Top-Most VLAN-ID策略在接口Inbound方向。

```
<H3C>display qos policy interface GigabitEthernet 5/0/3

  Interface: GigabitEthernet5/0/3

  Direction: Inbound

  Policy: uplink_1:2
   Classifier: uplink_1:2
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
     Behavior: uplink_1:2
      Nesting:
        Nest top-most vlan-id 10
```

③ 检查下行端口使能 QinQ。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看，确认在设备 GE5/0/3 端口使能 QinQ。

```
<H3C>display current-configuration interface GigabitEthernet 5/0/3
#
interface GigabitEthernet5/0/3
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 10 untagged
 qinq enable
 qos apply policy uplink_1:2 inbound
#
```

④ 检查下行端口允许 SVLAN 不携带 Tag 通过。

命令：*display interface interface-type interface-number*

例如：通过命令查看，确认设备 GE5/0/3 端口允许 SVLAN 10 报文不携带 Tag 通过。

```
<H3C>display interface GigabitEthernet 5/0/3
…
PVID: 1
 Mdi type: auto
 Link delay is 0(sec)
 Port link-type: hybrid
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1, 10
 Port priority: 0
 Last clearing of counters:  Never
…
```

（6）采用 2:2 VLAN MAPPING 方式

若采用 2:2 VLAN MAPPING 部署方式，请按照下列流量进行排查。

① 检查上行端口的上行策略配置正确。检查上行端口部署的上行策略中 Customer-VLAN-ID 为原报文的 CVLAN，Service-VLAN-ID 为修改后报文的 NEW_SVLAN，Customer-VLAN-ID 为修改后报文的 NEW_CVLAN。且策略中 Classifier 的 Operator 为 AND。注意，若仅修改原报文的 SVLAN，及不修改原报文的 CVLAN，可不配置该策略。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认 PE 设备与 PE 互联 GE5/0/4 端口部署的上行策略 Customer-VLAN-ID 为 100，Service-VLAN-ID 为 20，Customer VLAN ID 为 200 并且 Classifier 的 Operator 为 AND。

```
<H3C>display qos policy interface GigabitEthernet 5/0/4

  Interface: GigabitEthernet5/0/4

  Direction: Outbound

  Policy: upport_uplink_2:2
   Classifier: upport_uplink_2:2
```

```
          Operator: AND
          Rule(s) : If-match customer-vlan-id 100
                    If-match service-vlan-id 20
          Behavior: upport_uplink_2:2
           Marking:
             Remark Customer VLAN ID 200
```

② 检查下行端口的上行策略和下行策略配置正确。检查下行端口部署的上行策略中Customer-VLAN-ID为原报文的CVLAN，Service-VLAN-ID为原报文的SVLAN，Service VLAN ID为修改后报文的NEW_SVLAN。且策略中Classifier的Operator为AND。注意，若仅修改原报文CVLAN，及不修改原报文SVLAN，可不配置该策略。

检查下行端口部署的下行策略中Customer-VLAN-ID为修改后报文的NEW_CVLAN，Service-VLAN-ID为修改后报文的NEW_SVLAN，Customer-VLAN-ID为原报文的CVLAN（若下行端口的上行策略不修改原报文CVLAN，可不配置该策略），Service、VLAN、ID为原报文的SVLAN（若下行端口的上行策略不修改原报文SVLAN，可不配置该策略）。且策略中Classifier的Operator为AND。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认PE设备与CE互联GE5/0/5端口部署的上行策略downport_uplink_2:2中Customer-VLAN-ID为100，Service-VLAN-ID为10，Service-VLAN-ID为20。并且Classifier的Operator为AND。

通过命令查看，确认PE设备与CE互联GE5/0/5端口部署的下行策略downport_downlink_2:2中Customer-VLAN-ID为200，Service-VLAN-ID为20，Customer-VLAN-ID为100，Service-VLAN-ID为10。并且Classifier的Operator为AND。

```
     <H3C>display qos policy interface GigabitEthernet 5/0/5

       Interface: GigabitEthernet5/0/5

       Direction: Inbound

       Policy: downport_uplink_2:2
        Classifier: downport_uplink_2:2
          Operator: AND
          Rule(s) : If-match customer-vlan-id 100
                    If-match service-vlan-id 10
          Behavior: downport_uplink_2:2
           Marking:
             Remark Service VLAN ID 20

       Direction: Outbound

       Policy: downport_downlink_2:2
        Classifier: downport_downlink_2:2
          Operator: AND
          Rule(s) : If-match customer-vlan-id 200
                    If-match service-vlan-id 20
          Behavior: downport_downlink_2:2
```

```
          Marking:
            Remark Customer VLAN ID 100
          Marking:
            Remark Service VLAN ID 10
```

③ 检查上行端口应用策略的方向正确。检查上行端口 Customer-VLAN-ID 策略部署在接口 Outbound 方向。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认 PE 设备与 PE 互联 GE5/0/4 端口部署的 Customer、VLAN、ID 策略在接口 Outbound 方向。

```
<H3C>display qos policy interface GigabitEthernet 5/0/4

  Interface: GigabitEthernet5/0/4

  Direction: Outbound

  Policy: upport_uplink_2:2
   Classifier: upport_uplink_2:2
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
               If-match service-vlan-id 20
     Behavior: upport_uplink_2:2
      Marking:
        Remark Customer VLAN ID 200
```

④ 检查下行端口应用策略的方向正确。检查下行端口上行策略和下行策略部署在接口正确的方向。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认 PE 设备与 CE 互联 GE5/0/5 端口部署的上行策略 downport_uplink_2:2 在接口 Inbound 方向，部署的下行策略 downport_downlink_2:2 在接口 Outbound 方向。

```
<H3C>display qos policy interface GigabitEthernet 5/0/5

  Interface: GigabitEthernet5/0/5

  Direction: Inbound

  Policy: downport_uplink_2:2
   Classifier: downport_uplink_2:2
     Operator: AND
     Rule(s) : If-match customer-vlan-id 100
               If-match service-vlan-id 10
     Behavior: downport_uplink_2:2
      Marking:
        Remark Service VLAN ID 20

  Direction: Outbound

  Policy: downport_downlink_2:2
```

```
    Classifier: downport_downlink_2:2
      Operator: AND
      Rule(s) : If-match customer-vlan-id 200
                If-match service-vlan-id 20
      Behavior: downport_downlink_2:2
       Marking:
         Remark Customer VLAN ID 100
       Marking:
         Remark Service VLAN ID 10
```

⑤ 检查下行端口允许 NEW_SVLAN 携带 Tag 通过。

命令：*display interface interface-type interface-number*

例如：通过命令查看，确认设备 GE5/0/5 端口允许 NEW_SVLAN 20 报文携带 Tag 通过。

```
<H3C>display interface GigabitEthernet 5/0/5
…
Link delay is 0(sec)
 Port link-type: trunk
  VLAN passing   : 1(default vlan)
  VLAN permitted: 1(default vlan), 20
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
 Last clearing of counters:   Never
…
```

(7) 采用 N:1 VLAN MAPPING 方式

若采用 N:1 VLAN MAPPING 部署方式，请按照下列流量进行排查。

① 检查上行策略配置正确。检查上行策略中 Mode 为 dot1q-tag-manipulation，Customer-VLAN-ID 包含 CVLAN，Service-VLAN-ID 为 SVLAN。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认 PE 设备与 CE 互联 GE5/0/7 端口部署的上行策略 Customer-VLAN-ID 为 100 到 110，Service-VLAN-ID 为 10。且 Mode 为 dot1q-tag-manipulation。

```
<H3C>display qos policy interface GigabitEthernet 5/0/7

  Interface: GigabitEthernet5/0/7

  Direction: Inbound

  Policy: uplink_N:1
   Classifier : uplink_N:1
     Mode   : dot1q-tag-manipulation
     Operator AND
     Rule(s): If-match customer-vlan-id 100 to 110
     Behavior uplink_N:1
      Marking:
        Remark Service VLAN ID 10
```

② 检查使能 DHCP Snooping 功能和 ARP Detection 功能。

命令：*display dhcp-snooping*

display arp detection

例如：通过命令查看，确认 PE 设备使能 dhcp snooping 功能，同时在 SVLAN 中使能 arp detection 功能。

```
<H3C>display dhcp-snooping
 DHCP Snooping is enabled.
…

<H3C>display arp detection
 ARP detection is enabled in the following VLANs:
 10
```

③ 检查下行端口应用策略的方向正确。检查下行端口 Inbound 方向部署上行策略。

命令：*display qos policy interface interface-type interface-number*

例如：通过命令查看，确认 PE 设备与 CE 互联 GE5/0/7 端口 Inbound 方向部署的上行策略。

```
<H3C>display qos policy interface GigabitEthernet 5/0/7

  Interface: GigabitEthernet5/0/7

  Direction: Inbound

  Policy: uplink_N:1
   Classifier   : uplink_N:1
     Mode      :dot1q-tag-manipulation
     Operator : AND
     Rule(s)   : If-matchcustomer-vlan-id 100 to 110
     Behavior : uplink_N:1
      Marking:
        RemarkService VLAN ID 10
```

④ 检查上行和下行端口 QinQ 配置正确。检查上行端口配置 qinq uplink 模式，下行端口配置 qinq downlink 模式。

命令：*display current-configuration interface interface-type interface-number*

例如：通过命令查看，确认在 PE 设备上行口 GE5/0/6 端口使能 QinQ Uplink 模式；PE 设备下行口 G5/0/7 端口使能 QinQ Downlink 模式。

```
<H3C>display current-configuration interface GigabitEthernet 5/0/6
 #
interface GigabitEthernet5/0/6
port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10
 qinq enable uplink
 dhcp-snooping trust
 arp detection trust
```

```
#
<H3C>display current-configuration interface GigabitEthernet 5/0/7
#
interface GigabitEthernet5/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 10 100 to 110
 qinq enable downlink
 qos apply policy uplink_N:1 inbound
#
```

⑤ 检查上行端口使能 DHCP-Snooping Trust 和 ARP Detection Trust 功能。PE 设备上行端口需要设定为 DHCP-Snooping Trust 接口和 ARP Detection Trust 接口。

命令：*display dhcp-snooping trust*

display arp *detection statistics*

例如：通过命令查看，确认在 PE 设备上行口 GE5/0/6 端口使能 DHCP-Snooping Trust 和 ARP Detection Trust 功能。

```
<H3C>display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                    Trusted
 ----------------------------                --------------
 GigabitEthernet5/0/6

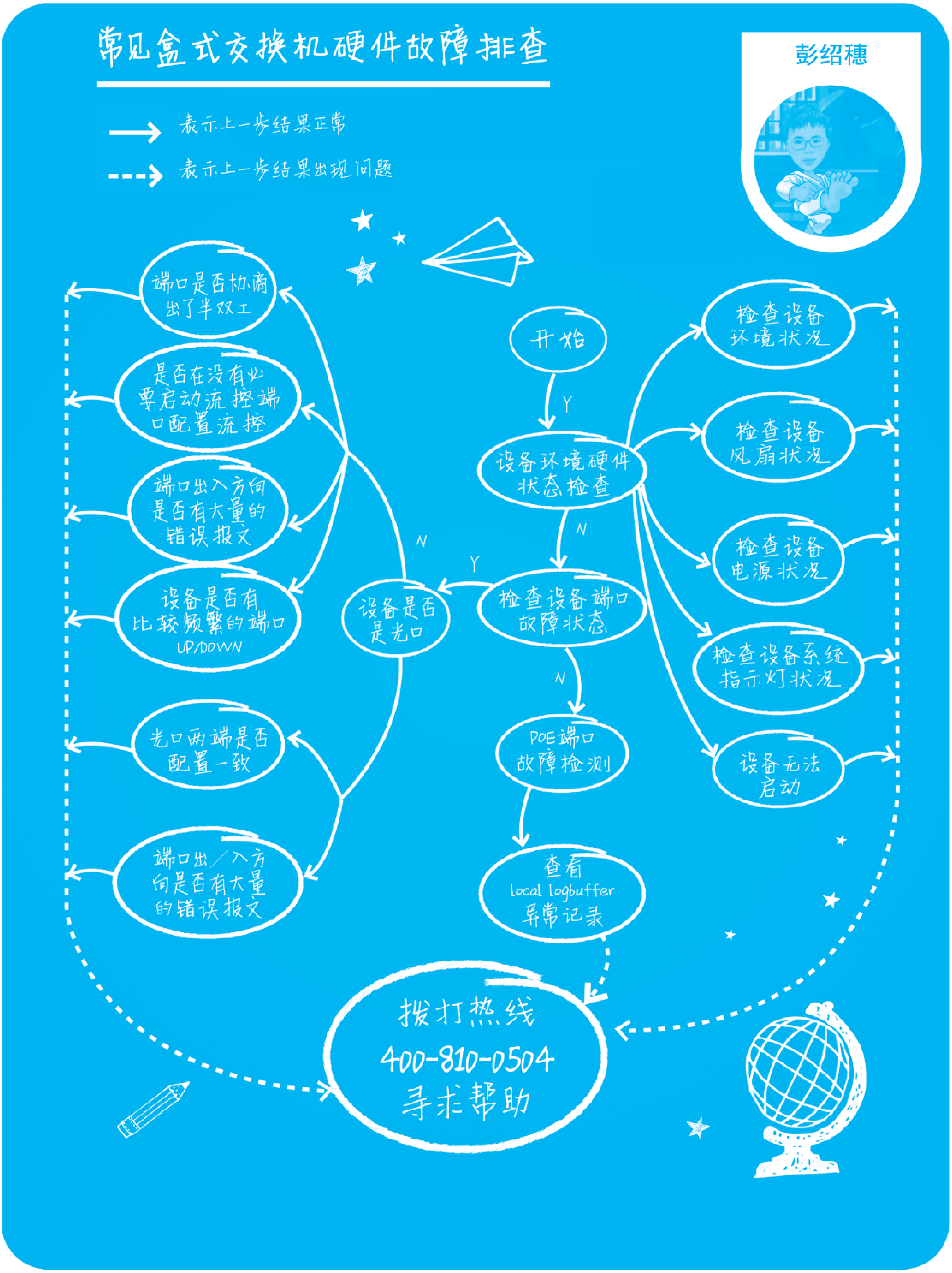
<H3C>display arp detection statistics
State: U-Untrusted   T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP          Src-MAC        Dst-MAC        Inspect
...
GE5/0/5(U)                0           0              0              0
GE5/0/6 (T)               0           0              0              0
GE5/0/7(U)                0           0              0              0
...
```

⑥ 检查下行端口允许 CVLAN 和 SVLAN 携带 Tag 通过。

命令：*display interface interface-type interface-number*

例如：通过命令查看，确认设备 GE5/0/7 端口允许 CVLAN 100 到 110 和 SVLAN 10 携带 Tag 通过。

```
<H3C>display interface GigabitEthernet 5/0/7
...
Link delay is 0(sec)
 Port link-type: trunk
  VLAN passing   : 1(default vlan), 10
  VLAN permitted: 1(default vlan), 10, 100-110
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0...
```


常见盒式交换机硬件故障排查
彭绍穗
表示上一步结果正常
表示上一步结果出现问题
开始
Y
设备环境硬件状态检查
检查设备环境状况
检查设备风扇状况
检查设备电源状况
检查设备系统指示灯状况
设备无法启动
N
检查设备端口故障状态
Y
N
设备是否是光口
端口是否协商出了半双工
是否在没有必要启动流控端口配置流控
端口出入方向是否有大量的错误报文
设备是否有比较频繁的端口UP/DOWN
光口两端是否配置一致
端口出/入方向是否有大量的错误报文
N
POE端口故障检测
查看local logbuffer异常记录
拨打热线
400-810-0504
寻求帮助

1. 开始

定位故障思路是：对于常见的设备硬件故障问题的判断，可以分为几个部分去检查，包括设备环境的硬件状态检查、端口故障状态的硬件检查、PoE 端口故障、local logbuffer 的异常记录来判断设备是否存在硬件故障。

2. 流程图相关操作说明

(1) 设备环境硬件状态检查

① 检查设备环境状况。

命令：*display environment*

```
<Sysname> display environment
System temperature information (degree centigrade):

--------------------------------------------------------------------------------

Sensor        Temperature   LowerLimit   WarningLimit   AlarmLimit ShutdownLimit

hotspot 1        44              5             70            80          NA

hotspot 2        37            -10            125           135          NA
```

Temperature 指的是当前温度，Lower Limit 指的是温度传感器的低温告警门限，Warning Limit 指的是温度传感器的一般级(Warning)高温告警门限。各传感器温度应处于低温告警门限与一般级高温告警门限之间，如出现异常温度告警，比如−1℃、255℃等，一般是软件版本问题或温度传感器硬件故障，需要更换设备。

② 检查设备风扇状况。

命令：*display fan*

```
<Sysname> display fan

Slot 1

      FAN      1

      State      : Normal
```

State 表示的是风扇的状态，风扇应该显示 Normal。如出现 Fault 或 Absent，如果风扇可以插拔，建议重新插拔后尝试，如问题仍然存在，建议更换风扇。如果风扇不能插拔，则建议直接更换整机。

③ 检查设备电源状况。

命令：*display power*

```
<Sysname> display power

Slot 1
```

```
Power    1
State    : Normal
Type     : AC
```

State 表示的是电源的状态，电源状态应该显示 Normal。如出现 Fault 或 Absent，如果电源可以插拔，建议重新插拔后尝试，如问题仍然存在，建议更换电源。如果电源不能插拔，则建议直接更换整机。

④ 检查设备系统指示灯状况。观察设备的系统状态指示灯的运行状况如表 5-7 所示。

表 5-7 系统状态指示灯

面板标识	指示灯状态	指示灯含义
SYS/PWR	绿色常亮	交换机已经正常启动
	绿色闪烁(1Hz)	系统正在上电自检
	红色常亮	系统上电自检失败、故障
	黄色闪烁(1Hz)	部分端口上电自检失败、功能失效
	灭	交换机断电

系统指示灯状态如果是绿色常亮和绿色闪烁即为正常启动或者系统正在上电，视为正常；如果出现红色常亮、绿色闪烁即为硬件故障，可以进行相应的更换。

⑤ 设备无法正常启动。用 Console 线，连接设备串口。在设备开始启动的时候，按 Ctrl+B 键进入 bootrom 菜单，检查启动文件是否存在，启动文件大小是否完全正确。如果版本文件正确，在设备开始启动的时候，按 Ctrl+T 键进行内存检测。

命令：*Ctrl+B*

Ctrl+T

```
1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modifybootrom password
6. Enterbootrom upgrade menu
7. Skip current configuration file
8. Setbootrom password recovery
9. Set switch startup mode
0. Reboot

Enter yourchoice(0-9):
```

选择 3 查看启动文件，并检查文件大小是否正确，如果文件不存在或者是文件大小不一致，建议重新通过 FTP/TFTP 导入 app 文件重新启动。如果文件大小正确，在设备开始启动的时候，按 Ctrl+T 键进行内存检测。如果出现内存检测失败，则直接更换设备。

(2) 检查设备端口故障状态

检查端口状态是否故障。

(3) 设备是否光口

判断端口是否是光口，如果不是光口按照步骤(2)①的流程进行分析判断；如果为光口，按照步骤(2)⑤的流程进行分析和判断。

① 端口是否协商出了半双工。

命令：*displayinterface brief*

例如：以 GigabitEthernet 1/0/2 端口为例。

```
<sysname>display interface brief

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down;Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
GE1/0/1            Down auto     A     H    1
GE1/0/2            Down auto     H     A    1
GE1/0/3            Down auto     A     A    1
GE1/0/4            Down auto     A     A    1
GE1/0/5            Down auto     A     A    1
GE1/0/6            Down auto     A     A    1
GE1/0/7            Down auto     A     A    1
GE1/0/8            Down auto     A     A    1
GE1/0/9            Down auto     A     A    1
GE1/0/10           Down auto     A     A    1
```

如果某个端口状态为 half，如 interface GigabitEthernet 1/0/2 duplex 为 half，则需要确认是否两端配置看下是否是因为配置不一致导致的双工状态为 half。

② 是否在没有必要启动流控端口配置流控。

命令：*display this*

例如：以 GigabitEthernet 1/0/2 端口为例。

```
[sysname-GigabitEthernet1/0/2]display this
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 duplex half
 flow-control
 loopback-detection enable
 loopback-detection action shutdown
#
return
```

如果某个端口不需要开启端口流控，查看该端口下是否配置了 flow-control，在不需要开启流控的端口可以通过命令 undo flow-control 来关闭流控配置来观察一下。

③ 端口出/入方向是否有大量的错误报文。

命令：*display interface interface-type interface-number*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> display interface GigabitEthernet 1/0/1
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
```

```
Input (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants,0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
-ignored, - parity errors
Output (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, -underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lostcarrier, - no carrier
```

检查设备的出入方向，是否有大量的错误报文，如果确实存在大量的错误包，检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。检查中间线路，如果有条件最好能够替换网线测试观察，看故障现象是否消失、错误报文是否还有增长。

④ 设备是否有比较频繁的端口 Up/Down。

命令：*display logbuffer*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<sysname>display logbuffer

%Apr 27 04:18:04:331 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Down.
%Apr 27 04:18:04:605 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Down.
%Apr 27 04:18:04:717 2000sysname IFNET/3/LINK_Up/Down: Vlan-interface1 link status is Down.
%Apr 27 04:18:04:859 2000sysname IFNET/5/LINEPROTO_Up/Down: Line protocol on the interface Vlan-interface1 is Down.
%Apr 27 04:18:08:706 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Up.
%Apr 27 04:18:08:818 2000sysname IFNET/3/LINK_Up/Down: Vlan-interface1 link status is Up.
%Apr 27 04:18:08:960 2000sysname IFNET/5/LINEPROTO_Up/Down: Line protocol on the interface Vlan-interface1 is Up.
%Apr 27 04:18:09:082 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Up.
%Apr 27 04:18:10:127 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Down.
%Apr 27 04:18:10:403 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Down.
```

查看设备的 logbuffer，检查设备是否存在频繁的端口的 Up/Down 信息。检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。修改下配置能否恢复，同时检查中间线路，如果有条件最好能够替换网线测试观察，看故障现象是否消失。

⑤ 光口两端是否配置一致。

命令：*display current-configuration interface*

```
<sysname>display current-configuration  interface
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
 voice vlan 30 enable
 lldp compliance admin-status cdp txrx
 lldp voice-vlan 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 duplex half
 flow-control
 loopback-detection enable
 loopback-detection action shutdown
#
```

检查当前端口的配置和对端的端口配置，是否存在配置不一致的情况，H3C 设备与其他厂商设备互连，建议光口速率和双工设置要完全一致。

⑥ 端口出/入方向是否有大量的错误报文。

命令：*display interface*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> display interface GigabitEthernet 1/0/1
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
-ignored, - parity errors
Output (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, -underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lostcarrier, - no carrier
```

检查设备的出入方向，是否有大量的错误报文，并且持续增长，如果确实存在大量的错误包，检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。检查中间线路，检查下光功率，看下是否处于临界值，如果有条件可以通过更换光模块、更换尾纤或清洗光模块连接器的方式解决。

(4) PoE 端口故障检测

命令：*poe enable*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1]poe enable
```

如设备本身是支持 PoE 的设备但却提示“PoE is not supported on the port”则说明 PoE 硬件存在问题，可尝试采用冷重启的方式重新复位看能否恢复，如不能恢复则可判断为 PoE 硬件故障。

（5）查看 local logbuffer 异常记录

命令：*en_diag*

local logbuffer display

```
<Sysname> system-view

[Sysname]en_diag

[Sysname_diag]local logbuffer display
```

如果在 local log 看到下列一致的报错，即可确定为硬件故障，其他故障可以联系 400 热线处理。

```
unit %d MMU channel 0 cell CRC error
unit %d MMU channel 0 packet CRC error
unit %d MMU channel 0 next pointer CRC error
unit %d MMU channel 0 pointer block CRC error
unit %d MMU channel 1 cell CRC error
unit %d MMU channel 1 packet CRC error
unit %d MMU channel 1 next pointer CRC error
unit %d MMU channel 1 pointer block CRC error
unit %d MMU ingress buffer overflow
unit %d MMU MSYS ingress buffer cell inconsistency
unit %d MMU IPMC pointer table parity error
unit %d MMU IPMC parity error if no table
unit %d MMU ingress statistics parity error
unit %d MMU fatal MCU FIFO error\n", unit
unit %d MMU fatal ASM FIFO error\n", unit
unit %d MMU possibly fatal ASM IGMU error
soc_fb_mmu_parity_error:unit = %d,"
                    "INTSTATUS  = 0x%08x Fail Count = %d\n",
unit = %d, CFAPFAILERROR
unit = %d, CFAPPARITYERRORPTR 0x%08x
unit = %d, MMU Soft Reset Error
unit = %d, MMU Cell not in progress
unit = %d, CBPCELLCRCERRPTR 0x%08x
unit = %d, CBPPKTHDRPARITYERRPTR 0x%08x
unit = %d, CBPCELLHDRPARITYERRPTR 0x%08x
unit = %d, XQPARITYERRORPBM 0x%08x
unit = %d, CCPPARITYERRORPTR 0x%08x
unit=%d, IPMC Over Pre-set Replication Limit
_soc_hx_ipipe_parity_error:unit = %d,"
"L2_ENTRY_PARITY_STATUS  = 0x%08x, "
                                "Bucket = %d Entry Bitmap 0x%02x\n"
Tucana MMU DRAM %s CRC error at 0x%08x
Tucana ARL parity analysis
```


高端交换机等价路由及链路聚合
出口流量负载不均故障排查
程 飞
表示上一步结果正常
表示上一步结果出现问题
开始
判定设备是否为PE设备的等价路由出口
确定LSP分担数目开启隧道策略，调整LSP负载分担数目
确定是否为IRF捻框出口
调整流量走向，使流量进入时就分担到不同IRF框上
判定是否为设备间二次hash
将上下级设备的hash因子错开
判定是否为本设备的二次hash
调整负载分担类型
抓包分析流量特点
拨打热线
400-810-0504
寻求帮助

1. 高端交换机等价路由及链路聚合出口流量负载不均故障排查

负载不均问题的主要排查思路如下。

① 判定设备是否为 PE 设备的等价路由出口。查看隧道策略的情况，开启隧道策略，调整 LSP 负载分担数目。

② 判定流量出口是否分步在 IRF 系统的不同框上，调整流量进入 IRF 系统时就分布到不同框上。

③ 判定是否为设备间二次 hash 情况，调整上下级设备的 hash 因子错开。

④ 判定是否为本设备的二次 hash，尝试升级或者直接联系 400 寻求帮助。

⑤ 判定只是普通的等价路由或者链路聚合，调整 hash 因子观察效果。

⑥ 如果调整后效果不好，通过抓包确定是否是由于现网流量自身特点导致的分担不均。

⑦ 上面的所有步骤都做了，依旧没有效果，收集信息并联系 400 寻求帮助。

2. 流程图相关操作说明

(1) 判定设备是否为 PE 设备的等价路由出口。

在这种组网下，现场情况如下。

可以看到私网路由已经等价。

```
<H3C> dis ip routing-tabl vpn-instance  unicom 119.34.128.0
Routing Tables:Unicom Destinations : 1019      Routes : 1998
Destination/Mask     Proto  Pre  Cost      NextHop       Interface
119.34.128.0/21      BGP    255  0         172.22.1.250  NULL0
                     BGP    255  0         172.22.1.250  NULL0
```

但是查看设备转发表里面，这条路由却并没有形成等价。

```
<H3C> dis fibvpn-instance unicom
Destination/Mask    Nexthop        Flag    OutInterface    InnerLabel    Token
119.34.128.0/21     172.22.1.250   UDG     NULL0           2087          2161
```

查看到目的地址的标签转发表也只有一个，因此流量不能负载均衡。

```
<H3C>dismpls nhlfe
Total NHLFE Entry: 60
Out-Interface    Token     Oper    Nexthop         Deep Stack
XGE8/0/1         2161      PUSH    172.22.0.229    1     1963
```

(2) 开启隧道策略，调整 LSP 负载分担数目

S125/95E 作为 PE 双上行的组网，若希望实现双上行 ECMP 负载分担，需要同步开启隧道策略，调整 LSP 负载分担数目，才能实现负载分担。默认情况下未使能 MPLS LSP 等价，如果存在多条 LSP，则优选先建立的 LSP，但可通过配置 tnl-policy 来实现 LSP 的等价。

```
[H3C]tunnel-policy 1
[H3C-tunnel-policy-1]tunnel select-seq lsp load-balance-number 2
[H3C]ip vpn-instance 1
[H3C-vpn-instance-1]tnl-policy 1
```

(3) 判定流量出口是否分步在 IRF 系统的不同框上

如果确定现场不是 PE 的等价路由设备,那么确定现场是否为 IRF 系统,流量出口是否分担到 IRF 系统的不同框上的出口。由于高端交换机具有本地优先转发的情况,从本框进入的流量,如果本框有出口,不管出口是链路聚合出口或者 ECMP 出口,都只会从本框优先转发,不会跨框转发。因此在这种情况下会出现出口流量不均的情况。

(4) 让进入 IRF 系统的流量分布到不同框上

只有在进入 IRF 系统之前调整流量走向,让流量分担到不同的框上转发。

说明:有一种情况例外,本框链路聚合+ECMP 的方式,即 IRF 系统是 ECMP 出口在不同的框,每个出口又是本框链路聚合出口,这种情况下不会本框优先转发,会跨框负载(如图 5-2 所示)。如果是这种情况,请往下排查。

(5) 判定是否为设备间二次 hash

设备间的二次 hash,指的是在上级设备进行了 ECMP 或者链路聚合后到达本设备,在设备再进行一次 ECMP 或者链路聚合。如图 5-3 所示,有两个等价路由链路出口,VOD3 到目的网段有两条等价路由,下一跳分别为 VOD1 和 VOD2,在 VOD1 和 VOD2 到目的网段分别也有两个等价路由,下一跳分别是 A 和 B,VOD4 和 VOD2 也是相同情况。在 VOD1 和 VOD2 上面流量始终只走了其中一条 ECMP 链路,另外一条链路流量很少或者基本上没有流量。

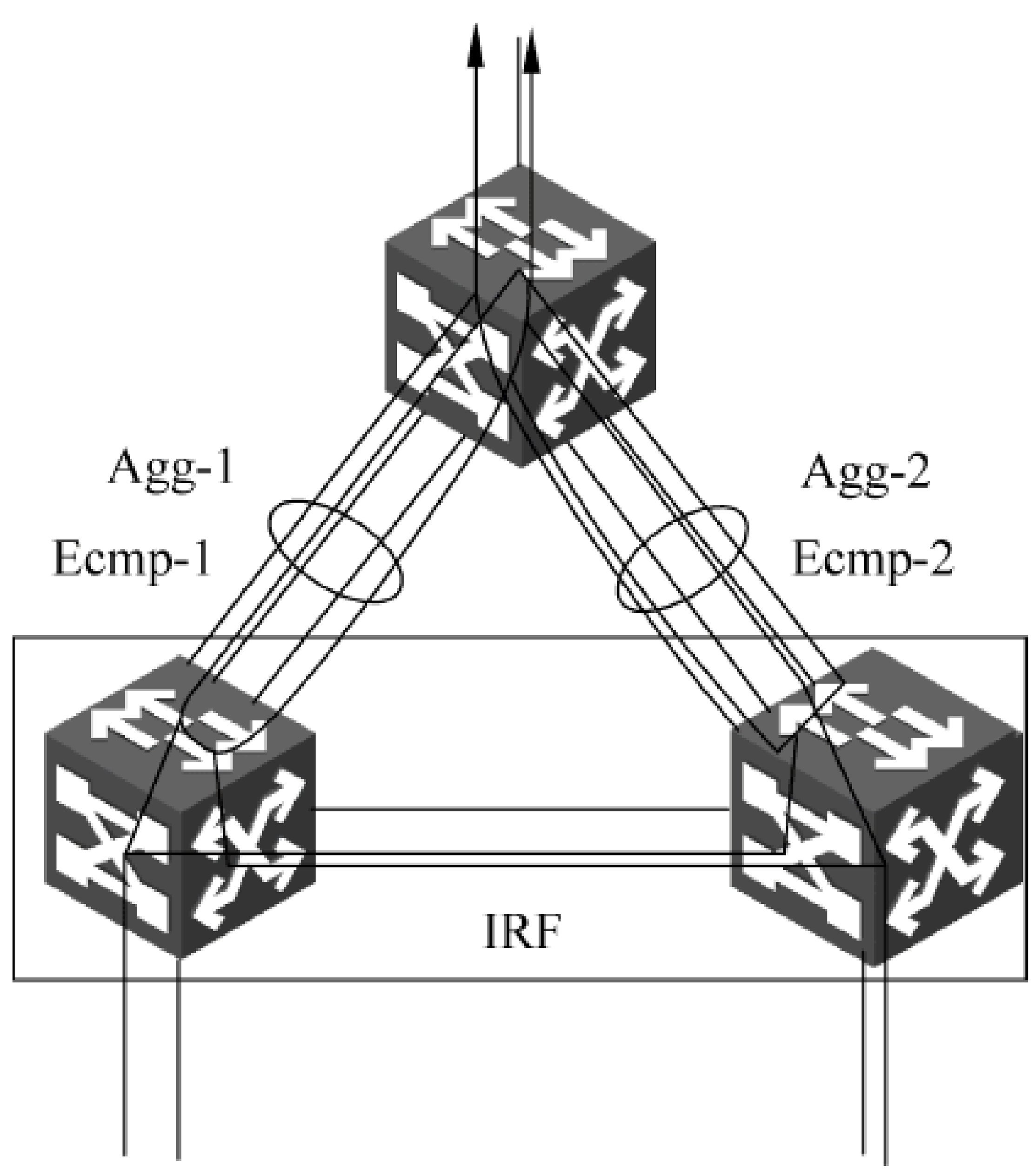


图 5-2 本框链路聚合+ECMP

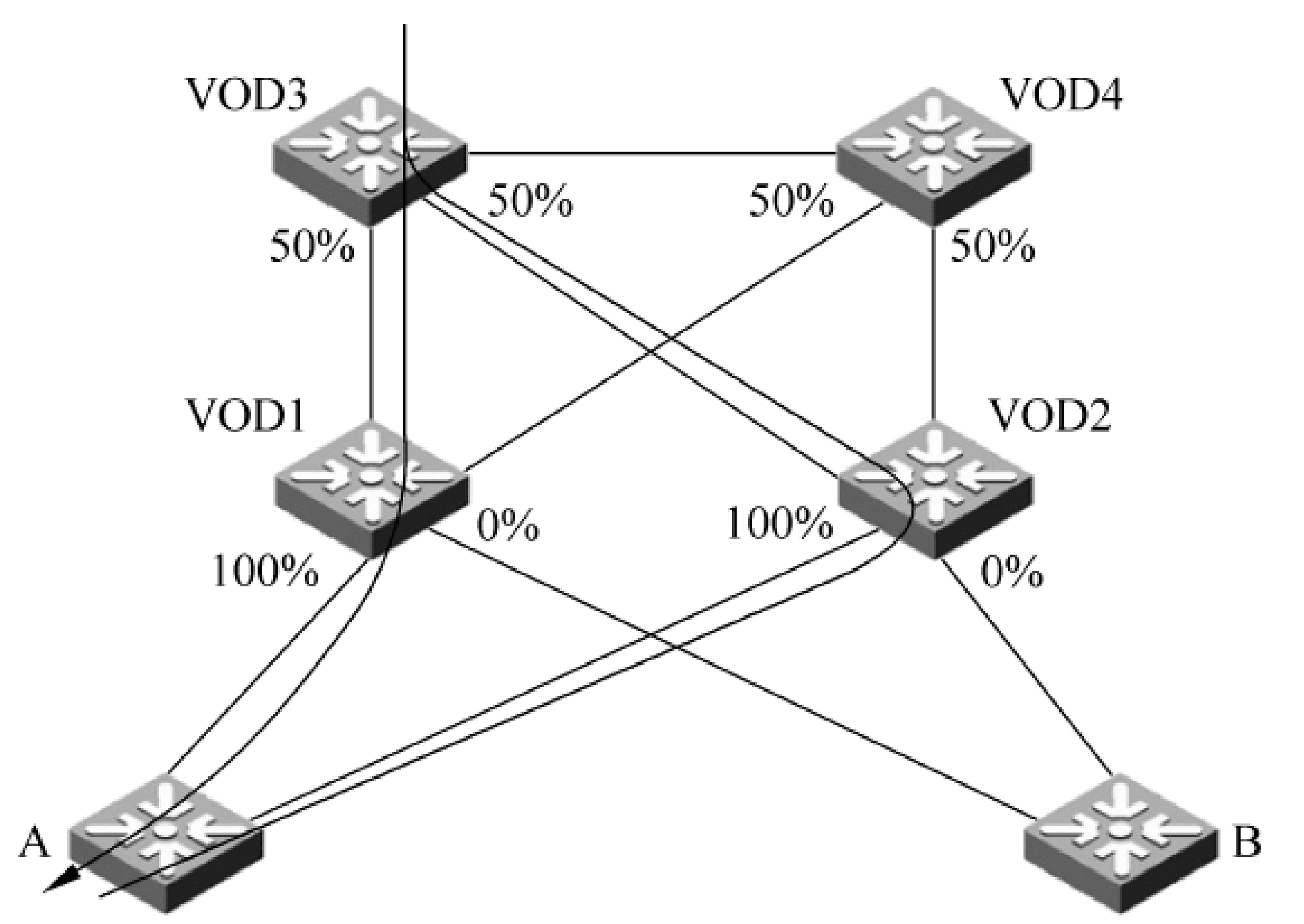


图 5-3 设备间二次 hash

在第一台设备进行过一次 hash 后,某些流被发到了 VOD1,其他流被发到了 VOD2;到了 VOD1 设备以后由于 VOD1 设备和 VOD3 设备用的是同样的 hash key,那么会出现某些 hash 因子偏少,某些 hash 因子偏多的情况,也就是从 VOD1 和 VOD2 设备出去的流量会非常不均匀。

(6) 将上下级设备的 hash 因子错开

可通过将两级设备 hash key 错开的方法来解决,例如第一级使用源地址、源端口,第二级使用目的地址、目的端口等。

```
VOD3/VOD4: link-aggregation load-sharing mode  source-ip source-port destination-ip destination-port
VOD1/VOD2: link-aggregation load-sharing  mode  source-ip  destination-ip
```

（7）判定是否为本设备的二次 hash

本设备的二次 hash，指的是本设备有 ecmp 出口，并且每个出口都是链路聚合出口。如图 5-4 所示，在这种组网下，也很容易出现流量负载不均的情况，原因和设备间二次 hash 的原因一致。

对于这种情况，解决方法如下。

① V5 版本：如果是 1828 之前版本（不含 1828）那么可以尝试升级到最新版本（最新版本对于聚合组内成员端口数小于等于 6 的情况做了一定优化）。

② V7 版本：如果是 7328 之前版本（不含 7328）那么可以尝试升级到最新版本。

最新版本聚合组内成员端口数小于等于 6 的情况做了一定优化；如果升级了仍然效果不明显，尝试用 ip load-sharing mode 命令调整逐流负载分担算法。

现场如果判定出了这种情况，可直接收集设备信息再拨打热线 400-810-0504 寻求帮助。

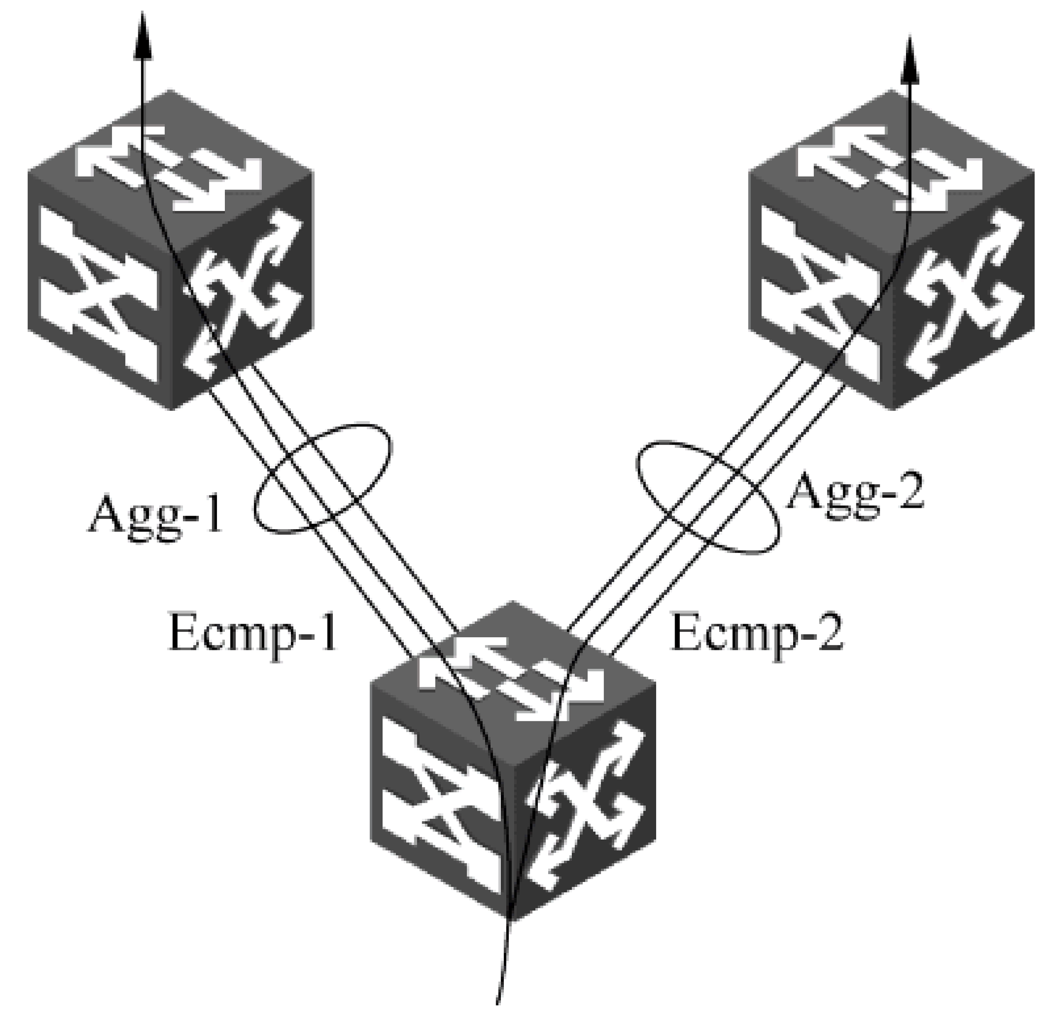


图 5-4　本设备的二次 hash

（8）调整负载分担类型

判断到这一步，已经可以确定为普通的等价路由出口或链路聚合出口。等价路由和链路聚合负载分担和两个因素有关：设备配置的负载分担类型；现网流量本身的变化情况。

解决方法：尝试调整设备的负载分担类型。

```
V5:link-aggregation load-sharing mode { destination-ip | destination-mac | destination-port | ingress-port | | mpls-label1 | mpls-label2 | mpls-label3 | source-ip | source-mac | source-port }

V7:link-aggregation global load-sharing mode { { destination-ip | destination-mac | destination-port | ingress-port | mpls-label1 | mpls-label2 | mpls-label3 | source-ip | source-mac | source-port } * | per-packet }
```

（9）抓包分析流量特点

如果试了各种负载分担类型还是分担不均，那么说明流量本身是不均匀的，建议抓包分析流量是现网流量自身特点导致的分担不均，如果本身某类流量就很多，hash 后该流量还是始终会 hash 到相同链路，所以这种情况下需要分析扩容是否可以对分担不均有改善。

如果流量模型没有某类流量大的情况，可直接收集设备信息再拨打热线 400-810-0504 寻求帮助。

高端交换机二次电源故障排查

程 飞





1. 开始

交换机二次电源故障指单板上的电源故障，故障后单板不能正常工作，主要排查思路如下。

① 判定设备接口板状态是否正常。

② 判定诊断信息中是否存在对应接口板的 poweroff 动作。

③ 判定 diagfile 中记录的 Hareware error，p2 的取值范围在 0～31 或大于等于 100。

④ 判定 diagfile 中记录问题时间点 a power down event 关键字。

⑤ 上面的所有步骤都做了，依旧没有效果，收集信息并联系 400 寻求帮助。

2. 流程图相关操作说明

(1) 判定设备接口板状态是否正常

交换机二次电源故障指单板上的电源故障，故障后单板不能正常工作，首先判断接口板状态。

```
<H3C>display device
Slot No.    Brd Type        Brd Status    Software Version
 0          LST1MRPNC1      Master        S12500-CMW520-R1828P04
 1          NONEAbsent      NONE
 2          LST1GT48LEC1    Normal        S12500-CMW520-R1828P04
 3          NONE            Off           NONE
```

如果该接口板显示状态为 Off 即可以认定为二次电源故障。

(2) 诊断信息中是否存在对应接口板的 poweroff 动作

按以下方式收集设备的诊断信息，并导出。

```
<H3C>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the filename(*.diag)[cfa1:/default.diag]:
Diagnostic information is outputting to cfa1:/default.diag.
Please wait...
Save successfully.
```

搜索诊断信息中的以下信息。

```
---------------------------------------------------------------------------
  --------------------Displaydevd board event of Slot 0--------------------
---------------------------------------------------------------------------
Slot  Flag  OldState  NewState SeqId    Date        Time
3     Power PowerOn ->PowerOff 2b15ccd 2014/09/01 16:16:51:705
3     Power PowerOn ->PowerOn 2b15cb7 2014/09/01 16:16:29:671
3     Power PowerOn ->PowerOn 2b15c2b 2014/09/01 16:14:08:257
3     Power PowerOn ->PowerOn 2b15b9f 2014/09/01 16:11:46:843
```

查看到诊断信息中有上面的 poweroff 记录则判定为二次电源故障。

(3) 排查 diagfile

排查 diagfile 中是否记录 Hardware error，p2 的取值范围是否在 0～31 或大于等于 100。

按以下方式收集设备 diagfile 信息，并导出。

```
[H3C]_hide
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]_diagnose-filesa
[H3C-hidecmd]_diagnose-filesave
Info: Save all the contents in the diagnostic file buffer into file cfa1:/diaglog/diagfile2.log successfully.
```

搜索 diagfile 信息中的以下信息。

```
%@3376660104 Sep 1 17:10:33:557 2014 S12508  DIAG/3/ERROR:0xcc180515 [1427]: Hardware
error! p1=3, p2=102
%@3376660105 Sep 1 17:10:33:557 2014 S12508  DIAG/3/ERROR:0xcc180515 [1427]: Hardware
error! p1=3, p2=103
%@3376660106Sep  1 17:10:33:557 2014 S12508  DIAG/3/ERROR:0xcc180515 [1427]: Hardware
error! p1=3, p2=104
%@3376660107Sep  1 17:10:33:557 2014 S12508  DIAG/3/ERROR:0xcc180515 [1427]: Hardware
error! p1=3, p2=106
%@3376660108Sep  1 17:10:33:557 2014 BJ-JX2F-C-S12508-48.Int  DIAG/3/ERROR:0xcc180515
[1427]: Hardware error! p1=3, p2=107
```

查看到 diagfile 信息中，有 Hardware error 记录，并且 p2 的取值范围大于了 100。有该记录则判定为二次电源故障。

（4）diagfile 中记录问题时间点 a power down event 关键字

查看到 diagfile 信息中有如上 power down event 记录则判定为二次电源故障。

```
%@4872 Sep 18 09:26:38:938 2014 S12500 Slot=3; SYSM/3/SYSM_NOTICE:0xcc000000
[367]: Board has experienced a power down event.
```

（5）更换单板

只要判断为二次电源故障，可以直接更换单板解决。

（6）以上信息均没有

如果更换单板后，单板依旧故障，或者无上述信息，则请打 400-810-0504 寻求帮助。

常见框式交换机硬件故障排查

彭绍穗





1. 开始

定位故障思路是：对于常见的设备硬件故障问题的判断，可以分为几个部分去检查，包括设备环境的硬件状态检查、端口故障状态的硬件检查、PoE 硬件故障、local logbuffer 的异常记录来判断设备是否存在硬件故障。

2. 流程图相关操作说明

(1) 设备环境硬件状态检查

① 检查设备环境状况。

命令：*display environment*

```
<Sysname> display environment

System temperature information (degree centigrade):

---------------------------------------------------------------------------
Slot   Sensor      Temperature  Lower  Warning  Alarm  Shutdown
0       inflow   1  25            0       80       97      NA
0       hotspot 1  38            0       80       97      NA
2       hotspot 1  31            0       75       92      NA
3       hotspot 1  34            0       75       92      NA
4       hotspot 1  43            0       75       92      NA
4       hotspot 2  55            0       88       100     110
6       hotspot 1  38            0       75       92      NA
```

Temperature 指的是当前温度，LowerLimit 指的是温度传感器的低温告警门限，WarningLimit 指的是温度传感器的一般级（Warning）高温告警门限。各传感器温度应处于低温告警门限与一般级高温告警门限之间，如出现异常温度告警，比如－1℃，255℃等，一般是软件版本问题或温度传感器硬件故障，需要更换单板。

② 检查设备风扇状况。

命令：*display fan*

```
<Sysname> display fan

Chassis 1:

 Fan       1 State: Normal

 Chassis   2:

 Fan       1 State: Normal
```

State 表示的是风扇的状态，风扇应该显示 Normal。如出现 Fault 或 Absent，建议重新插拔后尝试，如问题仍然存在，建议更换风扇。

③ 检查设备电源状况。

命令：*display power*

```
<Sysname> display power
 Power         0 State: Normal
 Power         1 State: Absent
 Power         2 State: Absent
 Power         3 State: Absent
```

State 表示的是电源的状态，电源状态应该显示 Normal。如出现 Absent，查看下电源开关是否打开或者电源输入是否正常接入，如出现 Fault 建议重新插拔后尝试，如问题仍然存在，建议更换电源。

④ 检查单板状态指示灯状况。观察单板的状态指示灯运行状况如表 5-8 所示。

表 5-8　单板的状态指示灯运行状况

单板状态指示灯状态		指示灯含义
RUN	ALM	
闪烁（1 次/秒）	灯灭	对应槽位单板正常工作
闪烁（1 次/秒）	闪烁（每 4 秒一次）	对应槽位单板温度异常（温度高于 Warning 高温门限或者温度低于低温告警门限）
常亮	常亮	对应槽位单板正在启动或者对应槽位单板故障
灯灭	灯灭	对应槽位单板不在位

检查主控板上，单板状态指示灯，如果 RUN 灯和 ALM 等常亮，可以主备倒换和替换单板槽位看下，如果现象依旧即为单板故障。

⑤ 单板状态异常。

命令：*Display device*

```
Slot Type          State    Subslot  Soft Ver       Patch Ver
 0   LSU1SUPA0     Master   0        S10500-0000    None
 1   NONE          Absent   0        NONE           None
 2   LSU1GP24TXSE0 Normal   0        S10500-0000    None
 3   LSU1GP48EB0   Normal   0        S10500-0000    None
 4   LSU1TGS32SF0  Normal   0        S10500-0000    None
 5   NONE          Absent   0        NONE           None
 6   LSU1FAB04A0   Normal   0        S10500-0000    None
 7   NONE          Absent   0        NONE           None
 8   NONE          Absent   0        NONE           None
 9   NONE          Absent   0        NONE           None
```

所有业务板应该是 Normal，主控板为 STANDBY、MASTER 状态，如果 display device 出现 Fault 或 Absent 状态，分析如下。

(a) 如果是新加入的主控板，同一设备两块主控板要求为同样型号，如不一致，需要更换解决、同一设备两块主控板要求使用同样版本，否则复发启动、重新上传相同的 app 文件启动、内存故障：使用备用主控板自身的 Console 口连接 Console 线，待主控板启动时使用 Ctrl+T 测试，如出现内存 FAIl 则内存故障，需要更换备用主控板。

(b) 如果出现业务板 Fault 或 Absent，故障点有主控板、机框、业务板，一般通过替换测试可以完全确定。如果双主控设备，可以通过主备倒换确认是否业务板在同一槽位的工作状况确认是否主控板问题，主备倒换后如业务板卡注册正常，则主控板故障肯定性最大。将该故障板卡替换到别的槽位，依旧无法启动，则业务板故障可能性最大。如果替换槽位能够正常启动，则可能是机框或者是主控板故障，可以替换主控板测试。

(2) 检查设备端口故障状态

判断端口是否是光口，如果不是光口，按照步骤(2)①的流程进行分析判断；如果为光口，按照步骤(2)⑤的流程进行分析和判断。

① 端口是否协商出了半双工。

命令：*display interface brief*

例如：以 GigabitEthernet 1/0/2 端口为例。

```
<sysname>display interface brief

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down;Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed    Duplex Type  PVID Description
GE1/0/1              Down auto     A      H     1
GE1/0/2              Down auto     H      A     1
GE1/0/3              Down auto     A      A     1
GE1/0/4              Down auto     A      A     1
GE1/0/5              Down auto     A      A     1
GE1/0/6              Down auto     A      A     1
GE1/0/7              Down auto     A      A     1
GE1/0/8              Down auto     A      A     1
GE1/0/9              Down auto     A      A     1
GE1/0/10             Down auto     A      A     1
```

如果某个端口状态为 half，如 interface GigabitEthernet 1/0/2 duplex 为 half，则需要确认是否两端配置看下是否是因为配置不一致导致的双工状态为 half。

② 是否在没有必要启动流控端口配置流控。

命令：*display this*

例如：以 GigabitEthernet 1/0/2 端口为例。

```
[sysname-GigabitEthernet1/0/2]display this
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 duplex half
```

```
flow-control
 loopback-detection enable
 loopback-detection action shutdown
 #
return
```

如果某个端口不需要开启端口流控，查看该端口下是否配置了 flow-control，在不需要开启流控的端口可以通过命令 undo flow-control 来关闭流控配置来观察一下。

③ 端口出/入方向是否有大量的错误报文

命令：*display interface interface-type interface-number*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> display interface GigabitEthernet 1/0/1
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants,0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
-ignored, - parity errors
Output (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, -underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lostcarrier, - no carrier
```

检查设备的出入方向，是否有大量的错误报文，如果确实存在大量的错误包，检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。检查中间线路，如果有条件最好能够替换网线测试观察，看故障现象是否消失、错误报文是否还有增长。

④ 设备是否有比较频繁的端口 Up/Down。

命令：*display logbuffer*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<sysname>display logbuffer

%Apr 27 04:18:04:331 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Down.
%Apr 27 04:18:04:605 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Down.
%Apr 27 04:18:04:717 2000sysname IFNET/3/LINK_Up/Down: Vlan-interface1 link status is Down.
%Apr 27 04:18:04:859 2000sysname IFNET/5/LINEPROTO_Up/Down: Line protocol on the interface Vlan-interface1 is Down.
%Apr 27 04:18:08:706 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Up.
%Apr 27 04:18:08:818 2000sysname IFNET/3/LINK_Up/Down: Vlan-interface1 link status is Up.
%Apr 27 04:18:08:960 2000sysname IFNET/5/LINEPROTO_Up/Down: Line protocol on the interface Vlan-interface1 is Up.
```

```
%Apr 27 04:18:09:082 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Up.
%Apr 27 04:18:10:127 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/10 link status is Down.
%Apr 27 04:18:10:403 2000sysname IFNET/3/LINK_Up/Down: GigabitEthernet1/0/16 link status is Down.
```

查看设备的 logbuffer，检查设备是否存在频繁的端口的 Up/Down 信息。检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。修改下配置能否恢复，同时检查中间线路，如果有条件最好能够替换网线测试观察，看故障现象是否消失。

⑤ 光口两端是否配置一致。

命令：*display current-configuration interface*

```
<sysname>display current-configuration interface
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
 voice vlan 30 enable
 lldp compliance admin-status cdp txrx
 lldp voice-vlan 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 duplex half
 flow-control
 loopback-detection enable
 loopback-detection action shutdown
#
```

检查当前端口的配置和对端的端口配置，是否存在配置不一致的情况，H3C 设备与其他厂商设备互连，建议光口速率和双工设置要完全一致。

⑥ 端口出/入方向是否有大量的错误报文。

命令：*display interface interface-type interface-number*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> display interface GigabitEthernet 1/0/1
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants,0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
-ignored, - parity errors
Output (total): 0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, - bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, -underruns, - buffer failures
```

```
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lostcarrier, - no carrier
```

检查设备的出入方向，是否有大量的错误报文，并且持续增长，如果确实存在大量的错误包，检查一下本端和对端的配置是相同，有没有存在一端配置为强制，一端配置为自动协商。检查中间线路，检查下光功率，看下是否处于临界值，如果有条件可以通过更换光模块、更换尾纤或清洗光模块连接器的方式解决。

(3) PoE 端口故障检测

命令：*poe enable*

例如：以 GigabitEthernet 1/0/1 端口为例。

```
<Sysname> system-view

[Sysname] interface GigabitEthernet 1/0/1

[Sysname-GigabitEthernet1/0/1]poe enable
```

如设备本身是支持 PoE 的设备但却提示“PoE is not supported on the port”则说明 PoE 硬件存在问题，可尝试采用冷重启的方式重新复位看能否恢复，如不能恢复则可判断为 PoE 硬件故障。

(4) 查看 local logbuffer 异常记录

命令：*en_diag*

local logbuffer display

```
<Sysname> system-view

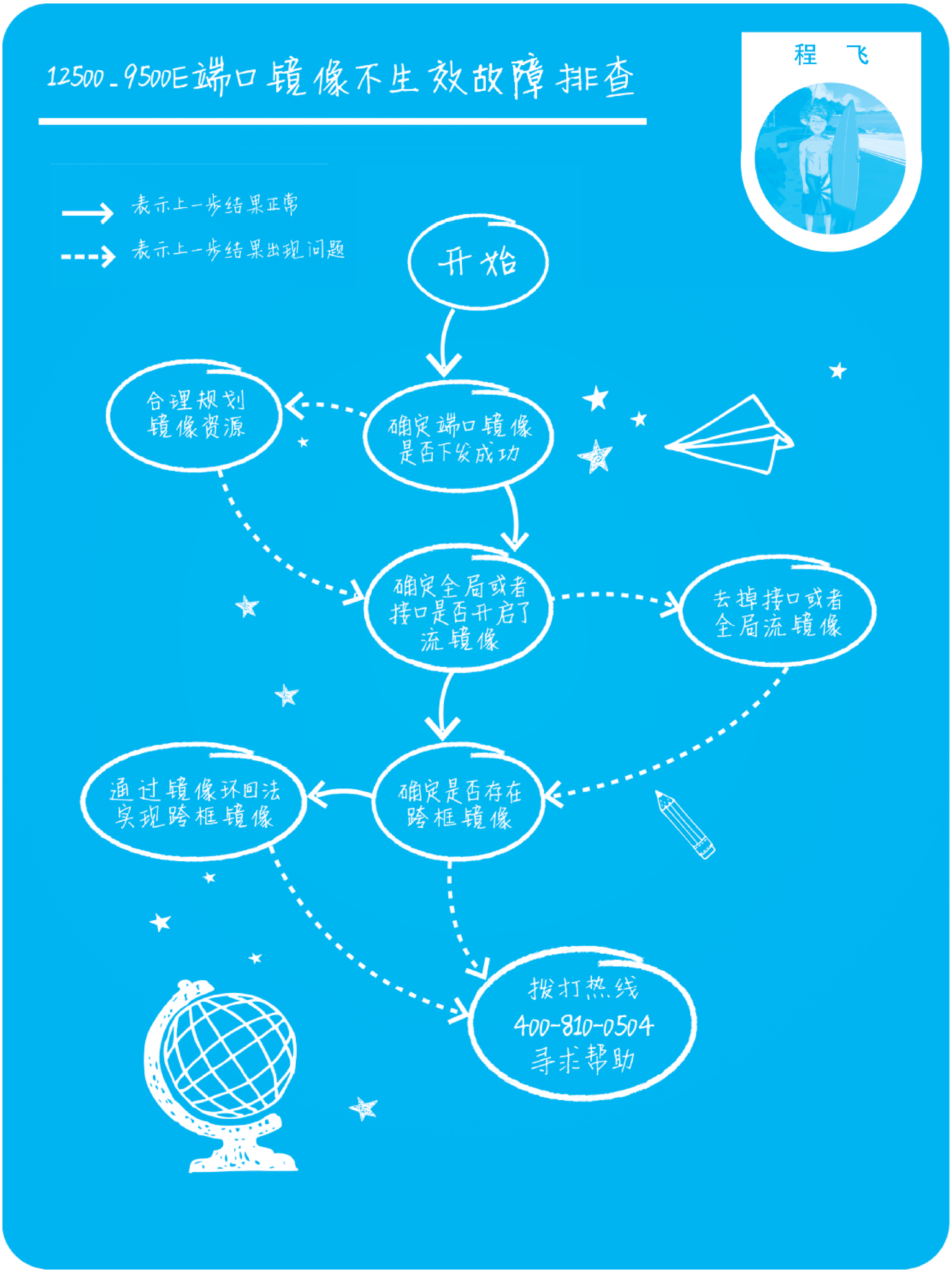
[Sysname]en_diag

[Sysname_diag]local logbuffer display
```

如果在 local log 看下下列一致的报错，即可确定为硬件故障，其他故障可以联系 400 热线处理。

```
unit %d MMU channel 0 cell CRC error
unit %d MMU channel 0 packet CRC error
unit %d MMU channel 0 next pointer CRC error
unit %d MMU channel 0 pointer block CRC error
unit %d MMU channel 1 cell CRC error
unit %d MMU channel 1 packet CRC error
unit %d MMU channel 1 next pointer CRC error
unit %d MMU channel 1 pointer block CRC error
unit %d MMU ingress buffer overflow
unit %d MMU MSYS ingress buffer cell inconsistency
unit %d MMU IPMC pointer table parity error
unit %d MMU IPMC parity error if no table
unit %d MMU ingress statistics parity error
unit %d MMU fatal MCU FIFO error\n", unit
unit %d MMU fatal ASM FIFO error\n", unit
unit %d MMU possibly fatal ASM IGMU error
```

```
soc_fb_mmu_parity_error:unit = %d,"
                    "INTSTATUS   = 0x%08x Fail Count = %d\n",
unit = %d, CFAPFAILERROR
unit = %d, CFAPPARITYERRORPTR 0x%08x
unit = %d, MMU Soft Reset Error
unit = %d, MMU Cell not in progress
unit = %d, CBPCELLCRCERRPTR 0x%08x
unit = %d, CBPPKTHDRPARITYERRPTR 0x%08x
unit = %d, CBPCELLHDRPARITYERRPTR 0x%08x
unit = %d, XQPARITYERRORPBM 0x%08x
unit = %d, CCPPARITYERRORPTR 0x%08x
unit=%d, IPMC Over Pre-set Replication Limit
_soc_hx_ipipe_parity_error:unit = %d,"
"L2_ENTRY_PARITY_STATUS = 0x%08x, "
                                  "Bucket = %d Entry Bitmap 0x%02x\n"
Tucana MMU DRAM %s CRC error at 0x%08x
Tucana ARL parity analysis
```


12500_9500E端口镜像不生效故障排查
程 飞
表示上一步结果正常
表示上一步结果出现问题
开始
确定端口镜像是否下发成功
合理规划镜像资源
确定全局或者接口是否开启了流镜像
去掉接口或者全局流镜像
确定是否存在跨框镜像
通过镜像环回法实现跨框镜像
拨打热线
400-810-0504
寻求帮助

1. 开始

端口镜像不生效排查思路如下。

① 确定端口镜像下发是否成功，端口镜像下发不生效的原因一般是超资源，因此要排查资源是否有超规格的情况。

② 排查接口或者全局是否存在流镜像的情况，如果有需要去掉全局或者接口流镜像。

③ 排查是否存在 IRF 系统中跨框镜像的情况，如果存在，则需要通过特殊配置方式实现客户跨框镜像需求。

④ 如果以上问题都不存在，那么收集信息，拨打 400-810-0504 寻求帮助。

2. 流程图相关操作说明

（1）排查端口镜像是否下发成功

通过下面 display mirroring-group 命令可以查看端口镜像是否可以下发成功。

可以看到镜像组 1 的状态是 active，镜像组 2 的状态是 inactive。那么可以确定镜像组 2 没有下发成功。一般没有下发成功的情况有可能是超过镜像资源了。

```
[H3C]dis mirroring-group all
mirroring-group 1:
    type: local
    status: active
    mirroring port:
        GigabitEthernet2/0/1    both
    mirroring VLAN:
    monitor port: GigabitEthernet2/0/47
mirroring-group 2:
    type: local
    status: inactive
    mirroring port:
        GigabitEthernet2/0/2    both
    mirroring VLAN:
    monitor port:
```

一个本地镜像组中可以配置多个镜像端口，即 mirroring-port；一个本地端口镜像组只能配置一个监控端口，即 monitor-port；一个监控端口只能属于一个镜像组；源 VLAN 镜像将会在所有的转发芯片上下发，端口镜像将会在端口所在转发芯片上下发；如果已经下发一个单方向 VLAN 镜像组后，芯片只剩下另一个方向的镜像资源来配置另一个方向的镜像组；如果已经下发双方向的 VLAN 镜像，那么芯片将没有更多资源配置其他镜像组。

（2）合理规划镜像资源

从上一排查步骤命令看出，g2/0/1 已经下发了一个镜像组了，然后 g2/0/2 又下发了一个另外一个镜像组，由于这两个接口共用同一个芯片，那么肯定只能下发成功一个镜像组。关于 12500-9500E 的镜像资源如下。

S9500E 产品端口镜像支持同方向的镜像组数量：①对于 24 个端口的 GE 单板，1 块单板只支持配置 1 个镜像组；②对于 48 个端口的 GE 单板（除了 LSR2GV48REB1 单板之外），

1个单板支持配置2个镜像组，其中前24个端口支持配置1个镜像组，后24个端口支持配置1个镜像组；③对于LSR2GV48REB1单板，1块单板只支持配置1个镜像组；④对于10GE单板(除了LSR1XP16REB1单板之外)，按照端口顺序，单板上每2个10GE端只支持配置1个镜像组；⑤对于LSR1XP16REB1单板，1个单板支持配置2个镜像组，按照端口顺序，前8个10GE端口支持配置1个镜像组，后8个10GE端口支持配置1个镜像组。

S12500产品端口镜像支持同方向的镜像组数量：①对于24个端口的GE单板，1块单板只支持配置1个镜像组；②对于48个端口的GE单板，1块单板支持配置2个镜像组，其中前24个端口支持配置1个镜像组，后24个端口支持配置1个镜像组；③对于10GE单板(除了LST1XP32REC1单板之外)，按照端口顺序，单板上每2个10GE端口只支持配置1个镜像组；④对于LST1XP32REC1单板，1个单板支持配置4个镜像组，按照端口顺序，前8个10GE端口支持配置1个镜像组，后8个10GE端口支持配置1个镜像组。

超过上述限制配置端口镜像组时，会报以下错误，这个可以在配置的时候注意一下报错情况。报错后的镜像组在display mirroring-group查看时就会显示成上面的inactive状态。如果出现这种情况，需要合理规划镜像资源，同一个芯片只能有一个镜像资源。

(3) 确定全局或者接口是否开启了流镜像

查看全局及接口是否配置了流镜像，如果全局或者接口配置了流镜像，并且匹配的流量和端口镜像的流量有重合，那么端口镜像的流量不会生效。如下显示，全局及接口都配置了流镜像，并且流镜像的报文匹配了所有，那么端口镜像的所有IP报文都镜像不到。

```
[H3C]dis qos policy  global
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: 1
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet2/0/45
[H3C]dis qos policy  interface  GigabitEthernet 2/0/1
  Interface: GigabitEthernet2/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior: 1
      Mirror enable:
        Mirror type: interface
        Mirror destination: GigabitEthernet2/0/45
[H3C]disacl  3000
AdvancedACL  3000, named -none-, 1 rule,
ACL's step is 5
 rule 0 permit ip
```

当镜像流量有重叠时，镜像的优先匹配顺序为：全局流镜像>接口流镜像>入方向端口镜像。由于流镜像不支持出方向，出方向端口镜像与流镜像不会重叠。

(4) 去掉接口或者全局流镜像

根据查看的结果，关闭掉全局或者端口下的流镜像。

```
[H3C]undo  qos apply policy 1 global inbound
[H3C-GigabitEthernet2/0/1]undo  qos apply policy 1 inbound
```

（5）确定是否存在跨框镜像

在 IRF2 模式下，S9500E/S12500 不支持流镜像到跨框的目的端口，且镜像到 VLAN 的流镜像只能镜像到本框，不能镜像给跨框端口。但是支持跨框镜像到 OAA 单板（例如，镜像到 NetStream 单板、重定向到 IPS/ACG 单板），同时在配置跨框流镜像到 OAA 单板的端口时，OAA 单板的端口必须包含在 VLAN 1 内，所以建议尽量不要在 VLAN 1 内配置其他业务，以免影响统计结果。因此需要确定现场是不是 IRF 的组网，并且同一个 mirroring-group 里面的 mirroring-port 及 monitor-port 是不是分布在不同的框上。

（6）通过镜像环回法实现跨框镜像

IRF2 模式下，12500/9500E 不支持跨框端口镜像和流镜像到跨框的目的端口，但支持流镜像到跨框的 OAA 插卡。解决跨框端口镜像，采用镜像环回法。

说明：跨框镜像的流量会占用 IRF 线路带宽，请提前规划，使得 IRF 线路有足够的带宽。

解决跨框端口镜像的配置举例如图 5-5 所示。

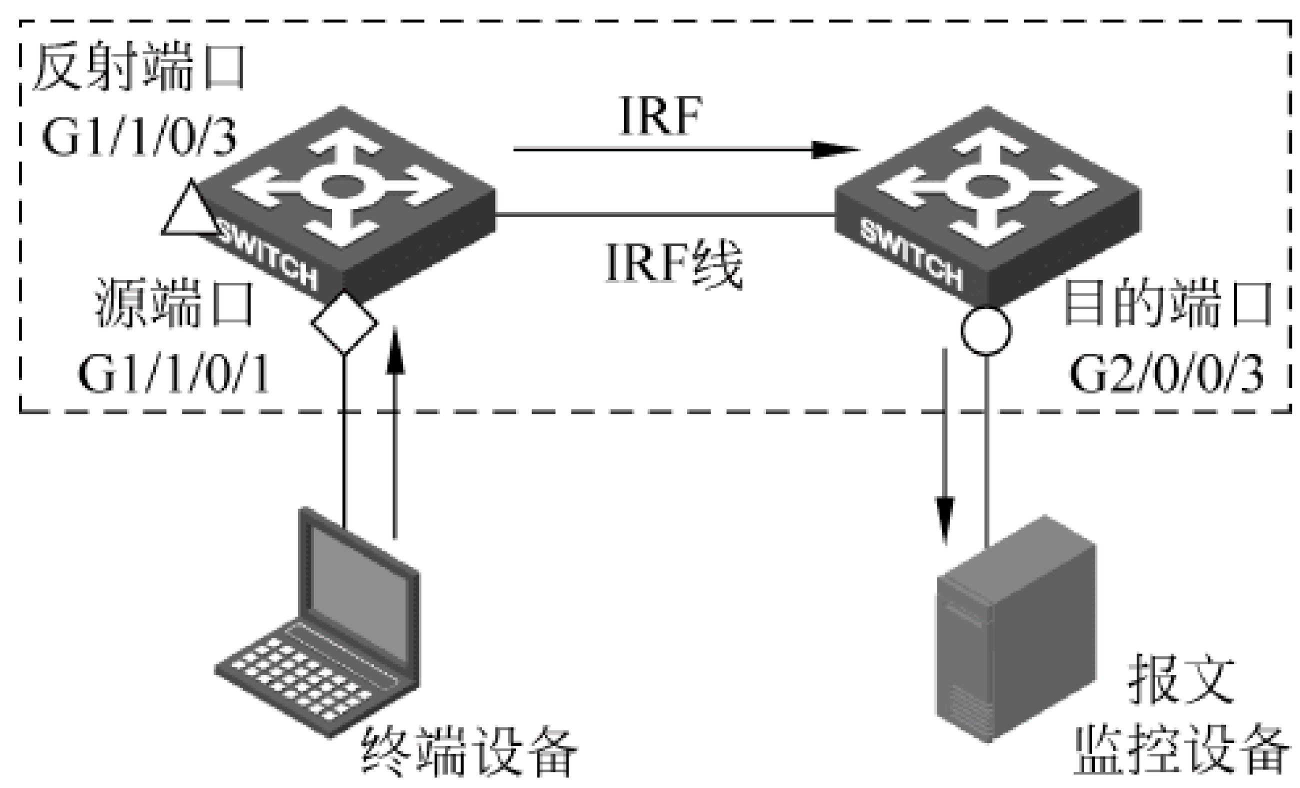


图 5-5　解决跨框端口镜像

```
//新建一个镜像 VLAN，该 VLAN 不能跑业务，只能用来传镜像报文
vlan 30
 mac-address max-mac-count 0
//配置端口镜像，把 mirroring-port 报文先镜像到环回口里面
mirroring-group 1 local
mirroring-group 1 mirroring-port GigabitEthernet 1/1/0/1
mirroring-group 1 moniter-port GigabitEthernet 1/1/0/3
//配置镜像环回口
interface GigabitEthernet1/1/0/3
 port access vlan 30
 loopback internal
 qinq enable
 mac-address max-mac-count 0
 stp disable
//把跨框的目的镜像端口加入到镜像 VLAN 30
interface GigabitEthernet2/0/0/3
 port access vlan 30
```

（7）收集信息

如果经过上面的排查后，依旧镜像不成功，收集诊断信息，诊断日志，日志文件，然后拨打 400-810-0504 反馈测试结果寻求帮助。


中低端交换机(V5)光口不能UP故障排查
张 磊
表示上一步结果正常
表示上一步结果出现问题
开始
排查两端光模块类型以及光纤是否匹配。
更换两端光模块型号及光纤型号
排查两端接口的端口速率和双工配置是否一致
修改接口的速率和双工配置
排查两端接口的收发光功率是否正常
替换光纤光模块替换测试
替换端口测试并收集信息
拨打热线
400-810-0504
寻求帮助

1. 开始

光口不能 Up 问题排查思路如下。

① 排查两端光模块类型以及光纤是否匹配,如果不匹配,请更换为一致。

② 排查两端接口的端口速率和双工配置是否一致,如果不一致,请更改为一致。

③ 排查两端的收发光功率是否正常。如果不正常,请替换光纤光模块测试。

④ 如果排查光模块、光纤以及传输设备都没问题,那可以通过更换端口来排查是否为端口自身问题,并同时收集信息,拨打 400-810-0504 寻求帮助。

2. 流程图相关操作说明

(1) 排查两端光模块类型以及光纤是否匹配

通过下面命令可以查看光模块类型。

```
[H3C]display transceiver interface GigabitEthernet 2/0/1
GigabitEthernet3/0/21 transceiver information:
  Transceiver Type                  : 1000_BASE_LX_SFP
  Connector Type                    : LC
  Wavelength(nm)                    : 1310
  TransferDistance(km)              : 10(9um)
  Digital DiagnosticMonitoring      : NO
  Vendor Name                       : H3C
  Ordering Name                     : SFP-GE-LX10-SM1310
```

两端的光模块类型需要匹配,本端是 SFP 的光模块,对端也必须是 SFP 的模块,如果对端是 SFP+的模块,那么是对接不成功的。

如果是多模模块,应该使用多模光纤;单模模块,使用单模光纤。多模和多模的判断可以看光纤表皮的标识,一般也可以通过颜色来简单判断,单模用黄色表皮,多模光纤一般用橙色的。

(2) 更换两端光模块型号及光纤型号

两端光模块需要匹配,有一点需要注意由于 SFP+(10GE)与 SFP(1GE)外形一样所以需要注意两者不要混用。确定光模块和光纤不匹配后,请更换成正确的型号。

(3) 排查两端接口的端口速率和双工配置是否一致

接口双工速率不一致,会造成接口不能 Up,所以需要排查两端接口双工及速率是否一致。

```
[H3C-GigabitEthernet2/0/1]dis int GigabitEthernet 2/0/1
GigabitEthernet2/0/1 current state: Down
Line protocol current state: Down
Description: GigabitEthernet2/0/1 Interface
The Maximum Transmit Unit is 1500
Link delay is 1(sec)
Internet protocolprocessing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0023-8911-7d01
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 0023-8911-7d01
Media type isoptical fiber, Port hardware type is 1000_BASE_LX_SFP
Loopback is not set
 1000 Mbps-speed mode, full-duplex mode
```

（4）修改接口的速率和双工配置

在接口下通过 duplex 和 speed 命令修改速率和双工配置。

```
interface GigabitEthernet2/0/1
 port link-mode route
 duplex full
 speed 1000
```

（5）排查两端接口的收发光功率是否正常

首先查看接口是否有收发光异常告警，可以通过查看光模块 alarm 信息来确认是本端问题还是光纤或者对端问题，alarm 信息查询命令。

```
<H3C>display transceiver alarm interface GigabitEthernet 2/0/1
GigabitEthernet2/0/1 transceiver current alarm information:
  RX power low
  RX loss of signal
```

通过上面命令显示，设备接口收光过低，可能是由于对端光模块发光低或者光纤有问题。可以通过查看两端接口光功率是否在正常范围之内。

本端可以看到收光功率为：－23.98，低于正常范围－22.08。

```
[H3C]_hide
[H3C-hidecmd]_distransceiver  diagnosis  interface  GigabitEthernet 2/0/1
GigabitEthernet2/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    32         3.35        9.32      -23.98         -5.56
  Alarm thresholds:
          Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High  73         3.60        40.83     -3.00          6.00
    Low   -3         3.00        1.00      -22.08         -12.50
```

怀疑对端发光低，因此查看对端发光功率，发现对端发光低。

```
[H3C-hidecmd]_distransceiver  diagnosis  interface  GigabitEthernet 1/0/10
GigabitEthernet1/0/10 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    34         3.36        9.54      -7.46          -14.06
  Alarm thresholds:
          Temp.(°C) Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High  73         3.60        41.64     -3.00          6.00
    Low   -3         3.00        1.00      -22.08         -12.50
```

（6）替换光纤光模块替换测试

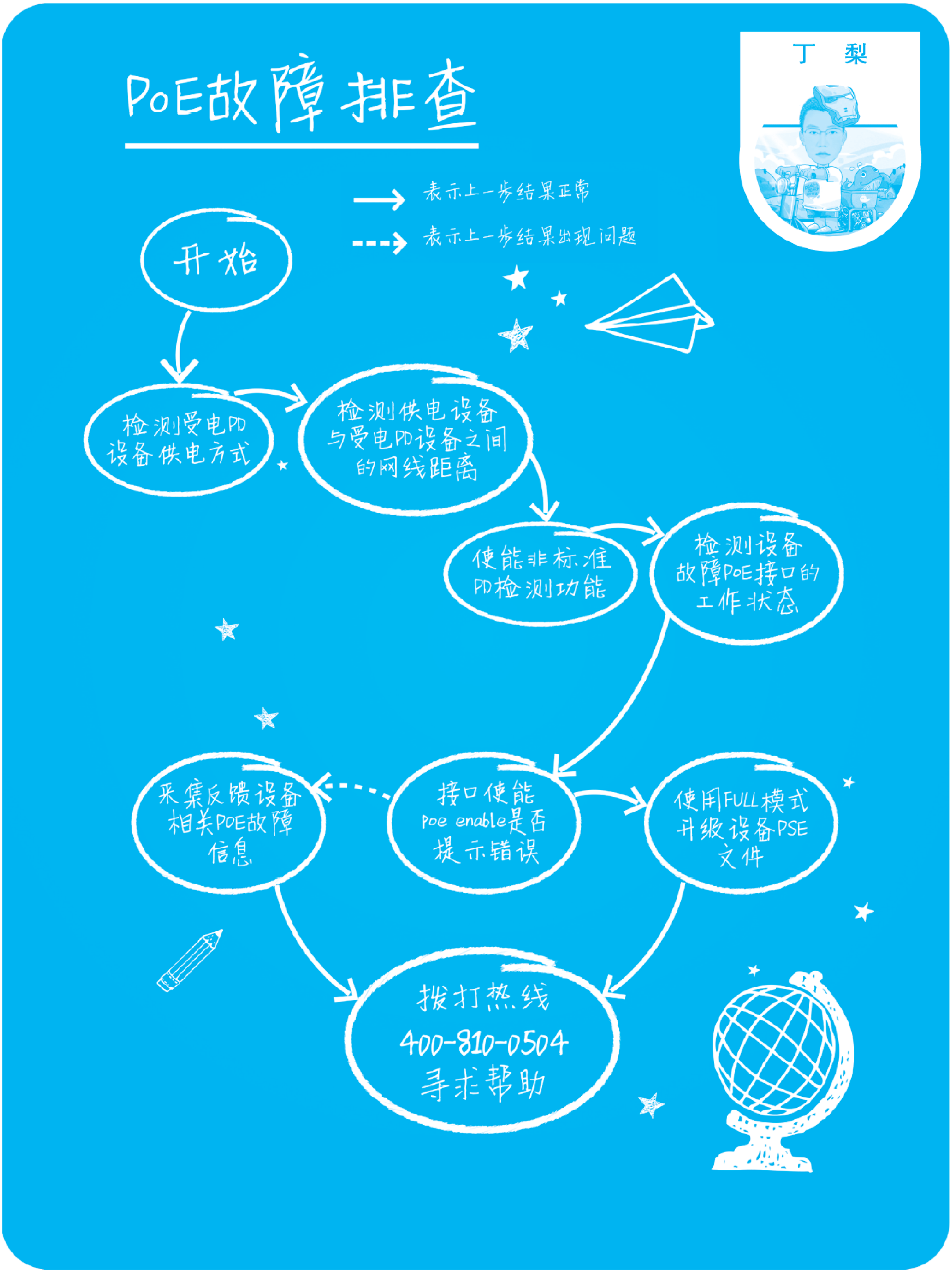
通过查看两端光功率情况，如果本端收光低，对端发光低，那么更换对端光模块测试；如果本端收光低，对端发光正常，怀疑是光纤异常，更换光纤测试，如果中间有传输设备，那么也排查一下传输设备是否有问题；如果本端发光低，那么更换本端光模块测试。

（7）替换端口测试并收集信息

如果更换了光模块光纤测试后，依旧异常，那么可以替换端口进行测试，然后收集诊断信

息及如下信息，然后拨打 400-810-0504 反馈测试结果并寻求帮助。

```
[H3C]display transceiver interface
[H3C]display transceiver alarm interface
[H3C]display transceiver manuinfo interface
[H3C]display transceiver diagnosis interface
[H3C-hidecmd]_display transceiver interface
[H3C-hidecmd]_display transceiver diagnosis interface
```


PoE故障排查
丁 梨
表示上一步结果正常
表示上一步结果出现问题
开始
检测受电PD设备供电方式
检测供电设备与受电PD设备之间的网线距离
使能非标准PD检测功能
检测设备故障PoE接口的工作状态
接口使能Poe enable是否提示错误
采集反馈设备相关POE故障信息
使用FULL模式升级设备PSE文件
拨打热线
400-810-0504
寻求帮助

1. 开始

定位故障的思路是：首先检查受电 PD 设备是否符合设备 PoE 供电要求，再检查设备 PoE 接口供电状态，最后根据使能 PoE 功能时的报错提示，收集并检查相关信息分析。

2. PoE 故障排查相关操作说明

（1）检测受电 PD 设备供电方式

检测对端受电的 PD 设备是空闲线供电还是信号线供电。目前我司交换机设备仅支持信号线供电方式。

> 信号线供电模式：PSE 使用 3/5 类双绞线中传输数据所用的线对(1、2、3、6)向 PD 传输数据的同时传输直流电。
>
> 空闲线供电模式：PSE 使用 3/5 类双绞线中没有被使用的线对(4、5、7、8)向 PD 来传输直流电。

（2）检测供电设备与受电 PD 设备之间的网线距离

建议供电设备与受电 PD 设备之前使用超 5 类及以上规格的双绞线，同时距离小于 100m。

（3）使能非标准 PD 检测功能

PD 设备分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 标准的 PD 设备。默认情况下，我司设备只能检测到标准 PD，并为其供电。只有在我司设备上时能检测非标准 PD 功能后，设备才能检测到非标准 PD，并为其供电。

命令：*poe legacy enable pse pse-id*

例如：通过命令使能设备非标准 PD 检测功能。

```
[H3C] poe legacy enable pse 10

PSE ID 的计算方法为：设备的成员编号×3＋1，例如：设备的成员编号为 3，其 PSE ID 为 3×3＋1
＝10
```

（4）检测设备故障 PoE 接口的工作状态

查看 PoE 接口工作状态，检测是否由于 PD 要求功率过大或供电设备剩余功率不足导致无法 PoE 供电。

命令：*display poe interface GigabitEthernet interface-number*

例如：通过命令查看 PoE 接口工作状态。

```
<H3C> display poe interface GigabitEthernet 1/0/1

 Port Power Enabled          : enabled

 Port Power Priority         : high

 Port Operating Status       : on

 Port IEEE Class             : 0
```

```
Port Detection Status          : delivering-power
Port Power Mode                : signal
Port Current Power             : 3600      mW
Port Average Power             : 3662      mW
Port Peak Power                : 3900      mW
Port Max Power                 : 15400     mW
Port Current                   : 71        mA
Port Voltage                   : 50.9      V
Port PD Description            :  IP Phone For Room 101
```

① Port Operating Status。

- off：供电功能禁用。
- on：正在正常供电。
- power-lack：PSE 剩余保证功率不够，导致无法对优先级为 Critical 的 PoE 接口供电。
- power-deny：拒绝供电，PD 要求功率大于配置功率。
- power-itself：外接设备正在自己供电。
- power-limit：正在受限供电，PD 要求功率大于配置功率，PSE 仍按配置功率供电。

② Port Detection Status。

- disabled：PoE 接口供电禁止。
- searching：正在搜索 PD。
- delivering-power：正在向 PD 供电。
- fault：错误。
- test：测试状态。
- other-fault：其他错误状态。
- pd-disconnect：PD 未连接。

(5) 接口使能 PoE enable 是否提示错误

设备接口使能 PoE enable 时是否提示错误。

```
[H3C]int Ethernet 1/0/1
[H3C-Ethernet1/0/1]poe enable
 PoE is not supported on the port!
```

(6) 使用 FULL 模式升级设备 PSE 文件

如果在接口上使能 PoE 功能时提示错误，请使用 FULL 模式升级 PSE 处理软件。

命令：*poe update full filename pse pse-id*

例如：升级 S5120-EI 交换机 PSE 处理软件。

```
[H3C] poe update full 00061204_0384_001_h3c.s19 pse 4
This command will refresh firmware on the specific PSE(s), Continue? [Y/N]: y
```

```
System is downloading firmware into the hardware. Please wait ...
 Update success
#
```

说明：升级所需要的 PSE 处理软件请联系 400 售后获取。

(7) 采集反馈设备相关 PoE 故障信息

如果接口使能 PoE 功能时没有提示错误，请收集如下信息后，反馈给 400 售后工程师。

```
(1) 收集故障时设备上 PoE 状态信息。
  <H3C>dis power
  <H3C>dis poe device
  <H3C>dis poe pse
  <H3C>dis poe interface 和 dis poe int gx/x/x(故障的端口和正常的端口都收集)
  <H3C>dis poe interface power
  <H3C>sys
  [H3C] en_diag
  [H3C-diagnose] debug poe dimm-status unit_id(非 IRF 设备默认 unit_id 为 1)
  [H3C-diagnose] debug poe port-power unit_id
  [H3C-diagnose] debug poe pse-info unit_id
  [H3C-diagnose] debug poe sys-status unit_id

(2) 收集故障时设备的诊断信息。
  <H3C>dis diag
```

高端交换机MQC重定向不生效故障排查

赵　跃



1. 开始

MQC 重定向不生效问题定位故障的思路是：先查看 ACL 规则是否匹配了流量，ACL 资源是否超规格，之后查看 MQC 重定向下一跳是否可达，最后查看是否配置 packet-filter/策略路由等功能，与 MQC 重定向冲突。

2. 流程图相关操作说明

(1) 查看 ACL 规则是否匹配流量

查看 ACL 规则的配置，确认 ACL 规则匹配了流量。

命令：*display acl acl-number*

例如：通过命令确认 ACL 规则是否匹配了需要做 MQC 重定向的流量。

```
<H3C>display acl 3000
AdvancedACL  3000, named -none-, 2 rules,
ACL's step is 5
 rule 0 permit ip source 10.0.0.0 0.0.0.255
 rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 100.0.0.0 0.0.0.255
```

(2) 修改/增加 ACL 规则

若通过 display acl 命令，查看规则中所写的 rule 规格错误，则需要重新下发 rule 命令，修改 rule 规则，确保 rule 规则匹配到流量。如果 ACL 中 rule 规则没有匹配所需做 MQC 重定向的流量，则需新增 rule 规则匹配该流量。

命令：*rule*

例如：ACL 规则中将需要做 MQC 重定向的源 IP 为 20.0.0.0/24、目的 IP 为 200.0.0.0/24 的流量错误写为源 IP 为 20.0.0.0/24、目的 IP 为 100.0.0.0/24，同时漏写源 IP 为 30.0.0.0/24 的流量，则需下发命令更正和增加 ACL 规则。

```
[H3C-acl-adv-3000]rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 200.0.0.0 0.0.0.255
Info: The rule id already exists, and the current operation is modifying the rule.
[H3C-acl-adv-3000]rule 10 permit ip source 30.0.0.0 0.0.0.255
[H3C-acl-adv-3000]display this
#
acl number 3000
 rule 0 permit ip source 10.0.0.0 0.0.0.255
 rule 5 permit ip source 20.0.0.0 0.0.0.255 destination 200.0.0.0 0.0.0.255
 rule 10 permit ip source 30.0.0.0 0.0.0.255
#
return
[H3C-acl-adv-3000]
```

(3) 检查 ACL 资源是否超规格

查看单板 ACL 资源利用情况，判断 ACL 资源是否已被耗尽，导致下发的 ACL 规则实际没有生效。

V5 平台命令：*display acl resource*

V7 平台命令：*dis qos-acl resource*

例如：通过下发命令查看，各个槽位单板 ACL 资源利用情况。

① V5。

```
<H3C>display acl resource
Interface:
 GE2/0/1 to GE2/0/24
---------------------------------------------------------------------
 Type          Total        Reserved      Configured  Remaining    Usage
---------------------------------------------------------------------
 ACL rule      2048         0             1978        70           96%
 Inbound ACL   2048         0             1978        70           96%
 OutboundACL   2048         0             70          0%

Interface:
   XGE3/0/1 to XGE3/0/2
---------------------------------------------------------------------
 Type          Total        Reserved      Configured  Remaining    Usage
---------------------------------------------------------------------
 ACL rule      8192         96            3           8093         1%
 Inbound ACL   8192         96            3           8093         1%
 OutboundACL   8192         0             0           8093         0%

 Interface:
   XGE3/0/3 to XGE3/0/4
---------------------------------------------------------------------
 Type          Total       Reserved     Configured   Remaining    Usage
---------------------------------------------------------------------
 ACL rule      8192        96           3            8093         1%
 Inbound ACL   8192        96           3            8093         1%
 OutboundACL   8192        0            0            8093         0%
```

② V7。

```
[H3C]dis qos-acl resource   slot   2
Interfaces: GE2/0/1 to GE2/0/24
---------------------------------------------------------------------
Type              Total      Reserved    Configured   Remaining   Usage
---------------------------------------------------------------------
ACL rule          8192       96          6            8090        1%
Inbound ACL       8192       96          5            8090        1%
Outbound ACL      8192       0           1            8090        0%
IN-MQC-CAR        8192       0           0            8192        0%
IN-COMM-CAR       7168       0           0            7168        0%
IN-COUNT          8192       0           64           8128        0%
OUT-MQC-CAR       8192       0           64           8128        0%
OUT-COUNT         8192       0           64           8128        0%
```

ACL 资源是按芯片划分的，并且 Inbound/Outbound 方向共用芯片 ACL 资源。通过 display acl resource 命令可以看到所有槽位芯片 ACL 资源的利用情况，如上 V5 所示，2 槽位单板的 GE2/0/1 至 GE2/0/24 属于同一个芯片，2048 的 ACL 资源由这 24 个接口共用。从示例中看到 2 槽位单板 2048 的 ACL 资源已利用了 96%，已接近 ACL 资源耗尽，会导致涉及 ACL 下发的功能正常应用，包括 MQC 重定向的使用。而 3 槽位的 XG3/0/1 和 XG3/0/2 属于同一个芯片，共用 8192 的 ACL 资源，当前 ACL 资源利用率为 1%，ACL 资源充足。XG3/0/3 和 XG3/0/4 类似。V7 平台的情况一样。

(4) 检查 MQC 重定向下一跳是否可达

检查 MQC 重定向配置中下一跳是否可达,如查看接口状态、ARP 表项、路由表或 ping 测试。

命令: *display interface interface-type interface-number*

display arp x.x.x.x

display ip routing-table x.x.x.x

ping x.x.x.x

例如: MQC 重定向下一跳配置为 100.0.0.2,通过查看接口状态、ARP 表项、路由表或 ping 测试确定 MQC 重定向下一跳是否可达。

```
<H3C>display  interface GigabitEthernet 2/0/1
 GigabitEthernet2/0/1 current state: Up
 ...

<H3C>displayarp 100.0.0.2
                 Type: S-Static    D-Dynamic    A-Authorized    M-Multiport
IP Address        MAC Address    VLANID  Interface           Aging Type
100.0.0.2         0023-8911-7d00 100     GE2/0/1             N/A    D

<H3C>display ip routing-table 100.0.0.2
RoutingTable : Public
SummaryCount : 1

Destination/Mask     Proto   Pre   Cost         NextHop         Interface

100.0.0.0/24         Direct  0     0            100.0.0.1       Vlan100

<H3C>ping 100.0.0.2
  PING 100.0.0.2:56   data bytes, press CTRL_C to break
    Reply from 100.0.0.2: bytes=56 Sequence=0ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=1ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=2ttl=255 time=1 ms
    Reply from 100.0.0.2: bytes=56 Sequence=3ttl=255 time=2 ms
    Reply from 100.0.0.2: bytes=56 Sequence=4ttl=255 time=1 ms

  --- 100.0.0.2ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

(5) 排查下一跳不可达原因

MQC 重定向下一跳不可达,需要排查 ARP、STP、接口状态等问题。

(6) 检查设备是否配置了 packet-filter/策略路由等功能

当设备在相关视图下配置了 packet-filter 或策略路由功能,由于 packet-filter 和策略路由的优先级比 MQC 重定向高,因而 MQC 重定向下发不生效。需要结合所需做 MQC 重定向的流量 ACL 规则,对配置进行排查。

命令: *display packet-filter*

display policy-based-route tesc

例如：acl number 3000 匹配了所需做 MQC 重定向的流量，同时在设备上下发了 packet-filter/策略路由功能。packet-filter 可以在二/三层物理接口及三层虚接口上下发，设备上可以配置本地策略路由和接口策略路由，均需要排查。需注意，如下示例中，acl number 3000 同时作为 MQC 重定向、packet-filter、策略路由的感兴趣流量匹配条件，并且实际现网中可能存在不同 ACL，但是规则匹配相同的流量做 packet-filter/策略路由，也会造成 MQC 重定向不生效，因此需要排查不同的 ACL 中是否有相同的 rule 规则。

说明： 设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 之前的版本，QoS 策略的优先级高于策略路由，不涉及策略路由功能部分的排查。而设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 及之后的版本，QoS 策略的优先级低于策略路由，涉及策略路由功能部分的排查。

```
[H3C]dis packet-filter all
  Interface: Vlan-interface100
  In-bound Policy:
    acl 3000, Successful
  Out-bound Policy:
[H3C-Vlan-interface100]display this
#
interface Vlan-interface100
 ip address 100.0.0.1 255.255.255.0
 packet-filter 3000 inbound
#
return
#
traffic classifier test operator and
 if-match acl 3000
#
traffic behavior test
 redirect next-hop 100.0.0.2 fail-action forward
#
qos policy test
 classifier test behavior test
#
[H3C]dis policy-based-route
 Policy based routing configuration information:
 policy-based-route : test
    Node 1permit :
      if-match acl 3000
      apply ip-address next-hop 100.0.0.2

[H3C]interface Vlan-interface 10
[H3C-Vlan-interface10]display this
#
interface Vlan-interface10
 ip address 10.0.0.1 255.255.255.0
 ip policy-based-route test
#
return
#
ip local policy-based-route test
#
```

```
[H3C-GigabitEthernet2/0/1]dis this
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 100
 qos apply policy test inbound
```

（7）修改配置

通过上一步的排查发现 MQC 重定向与 packet-filter/策略路由同时下发，导致 MQC 重定向不生效，需修改配置。

① MQC 重定向与 packet-filter 同时下发的情况。包过滤下发在 Inbound 方向时，将导致 MQC 重定向感兴趣的流量在执行 MQC 重定向动作之前被过滤掉。包过滤下发在 Outbound 方向时，将导致 MQC 重定向动作执行完后，报文被过滤掉，流量仍无法按 MQC 重定向需求转发出去。在上述两种情况下，均需要在 packet-filter 的 ACL 规则中，将需要正常转发的流量 rule 规则去掉。

② MQC 重定向与策略路由同时下发的情况。MQC 重定向感兴趣的流量先由策略路由匹配后处理了。该种情况下，需重新了解和细化需求，是否可以通过细化 MQC 重定向 ACL 规则和策略路由 ACL 规则，使两个 ACL 规则不冲突，流量能区分出来按不同的功能执行动作。

说明： 设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 之前的版本，QoS 策略的优先级高于策略路由，不涉及策略路由功能部分的排查。而设备的软件版本为 S12500-CMW520-R1335/S9500E-CMW520-R1335 及之后的版本，QoS 策略的优先级低于策略路由，涉及策略路由功能部分的排查。

（8）收集信息

做了以上操作，还不能解决问题，请收集诊断信息、日志信息、诊断日志，然后拨打 400-810-0504 热线寻求帮助。


中低端交换机(V5)等价路由出口流量负载不均故障排查
张 磊
表示上一步结果正常
表示上一步结果出现问题
开始
确定设备是否为PE设备的等价路由出口
确定LSP分担数目开启隧道策略，调整LSP负载分担数目
确定是否为IRF跨框出口
链路聚合负载分担不均匀
ECMP负载分担不均匀
关闭LACP本地优先转发
调整流量走向，使流量进入时就分担到不同IRF框上
判定是否为设备间二次hash
将上下级设备的hash因子错开
调整负载分担类型
抓包分析流量特点
拨打热线
400-810-0504
寻求帮助

1. 开始

负载不均问题的主要排查思路如下。

① 判定设备是否为 PE 设备的等价路由出口。查看隧道策略的情况。开启隧道策略,调整 LSP 负载分担数目。

② 判定流量出口是否分步在 IRF 系统的不同框上;若是链路聚合则关闭聚合组的本地优先转发观察,若是 ECMP 分担不均匀,调整流量进入 IRF 系统时就分布到不同框上。

③ 判定是否为设备间二次 hash 情况,调整上下级设备的 hash 因子错开。

④ 判定是否为本设备的二次 hash,尝试升级或者直接联系 400 寻求帮助。

⑤ 判定只是普通的等价路由或者链路聚合,调整 hash 因子观察效果。

⑥ 如果调整后效果不好,通过抓包确定是否是由于现网流量自身特点导致的分担不均。

⑦ 上面的所有步骤都做了,依旧没有效果,收集信息并联系 400 寻求帮助。

2. 流程图相关操作说明

(1) 判定设备是否为 PE 设备的等价路由出口

在这种组网下,现场情况如下。

可以看到私网路由已经等价。

```
<H3C> display ip routing-table vpn-instance unicom 119.34.128.0
Routing Tables:Unicom Destinations : 1019       Routes : 1998
Destination/Mask     Proto  Pre  Cost     NextHop       Interface
119.34.128.0/21      BGP    255   0       172.22.1.250    NULL0
                     BGP    255   0       172.22.1.250    NULL0
```

但是查看设备转发表里面,这条路由却并没有形成等价。

```
<H3C> dis fibvpn-instance unicom
Destination/Mask    Nexthop        Flag    OutInterface    InnerLabel    Token
119.34.128.0/21     172.22.1.250   UDG      NULL0           2087          2161
```

查看到目的地址的标签转发表也只有一个,因此流量不能负载均衡。

```
<H3C>display mpls nhlfe
Total NHLFE Entry: 60
Out-Interface      Token        Oper      Nexthop          Deep Stack
XGE8/0/1           2161         PUSH      172.22.0.229     1      1963
```

(2) 开启隧道策略,调整 LSP 负载分担数目

交换机作为 PE 双上行的组网,若希望实现双上行 ECMP 负载分担,需要同步开启隧道策略,调整 LSP 负载分担数目,才能实现负载分担。默认情况下未使能 MPLS LSP 等价,如果存在多条 LSP,则优选先建立的 LSP,但可通过配置 tunnel-policy 来实现 LSP 的等价。

```
[H3C]tunnel-policy 1
[H3C-tunnel-policy-1]tunnel select-seq lsp load-balance-number 2
[H3C]ip vpn-instance 1
[H3C-vpn-instance-1]tnl-policy 1
```

（3）判定流量出口是否分步在 IRF 系统的不同框上

如果确定现场不是 PE 的等价路由设备，那么确定现场是否为 IRF 系统，流量出口是否分担到 IRF 系统的不同框上的出口。由于中低端交换机具有本地优先转发的情况，从本框进入的流量，如果本框有出口，不管出口是链路聚合出口或者 ECMP 出口，都默认只会从本框优先转发，不会跨框转发。因此在这种情况下会出现出口流量不均的情况。

（4）链路聚合负载分担不均匀

确认是否是链路聚合分担不均匀。

（5）关闭 LACP 本地优先转发

关闭链路聚合的本地优先转发。

```
<H3C>system-view
[H3C]undo link-aggregation load-sharing mode local-first
```

（6）ECMP 负载分担不均匀

确认是否是 ECMP 分担不均匀。

（7）让进入 IRF 系统的流量分布到不同框上

只有在进入 IRF 系统之前调整流量走向，让流量分担到不同的框上转发。

（8）判定是否为设备间二次 hash

设备间的二次 hash，指的是在上级设备进行了 ECMP 或者链路聚合后到达本设备，在设备再进行一次 ECMP 或者链路聚合。如图 5-6 所示情况，有两个等价路由链路出口，VOD3 到目的网段有两条等价路由，下一跳分别为 VOD1 和 VOD2，在 VOD1 和 VOD2 到目的网段分别也有两个等价路由，下一跳分别是 A 和 B，VOD4 和 VOD2 也是相同情况。在 VOD1 和 VOD2 上面流量始终只走了其中一条 ECMP 链路，另外一条链路流量很少或者基本上没有流量。

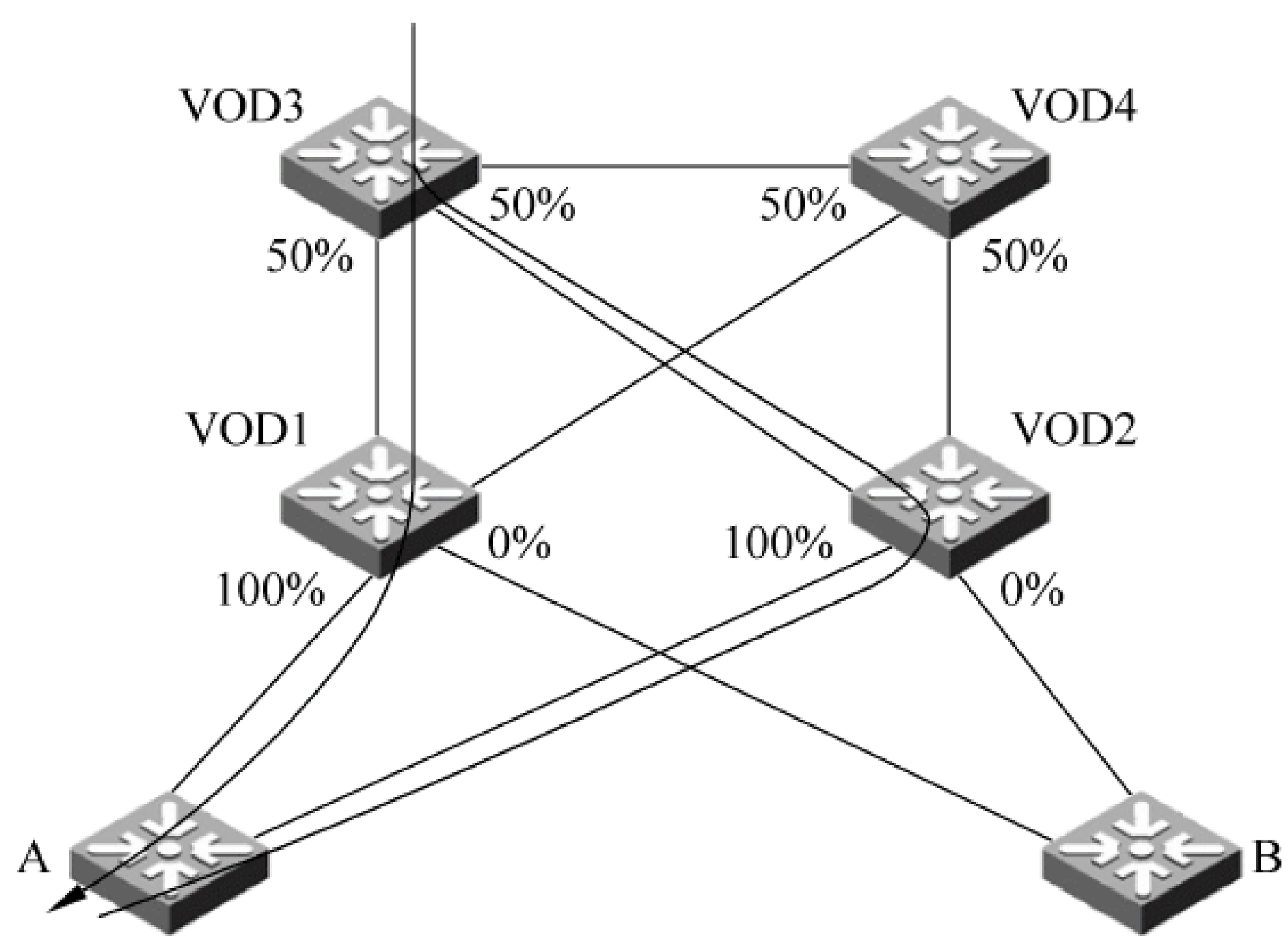


图 5-6　设备间二次 hash

在第一台设备进行过一次 hash 后，某些流被发到了 VOD1，其他流被发到了 VOD2；到了 VOD1 设备以后由于 VOD1 设备和 VOD3 设备用的是同样的 hash key，那么会出现某些 hash 因子偏少，某些 hash 因子偏多的情况，也就是从 VOD1 和 VOD2 设备出去的流量会非常不均匀。

（9）将上下级设备的 hash 因子错开

可通过将两级设备 hash key 错开的方法来解决，例如第一级使用源地址、源端口，第二级

使用目的地址、目的端口等。

```
VOD3/VOD4: link-aggregation load-sharing mode  source-ip source-port destination-ip destination-port
VOD1/VOD2: link-aggregation load-sharing    mode  source-ip  destination-ip
```

(10) 调整负载分担类型

判断到这一步,已经可以确定为普通的等价路由出口或链路聚合出口。等价路由和链路聚合负载分担和两个因素有关:设备配置的负载分担类型;现网流量本身的变化情况。

V5 设备上没有命令专门修改 ECMP 的 hash 因此,可以配置全局的 LACP 负载分担类型为源 IP、目的 IP、源端口、目的端口来使四层端口号来参与 ECMP 的链路分担。

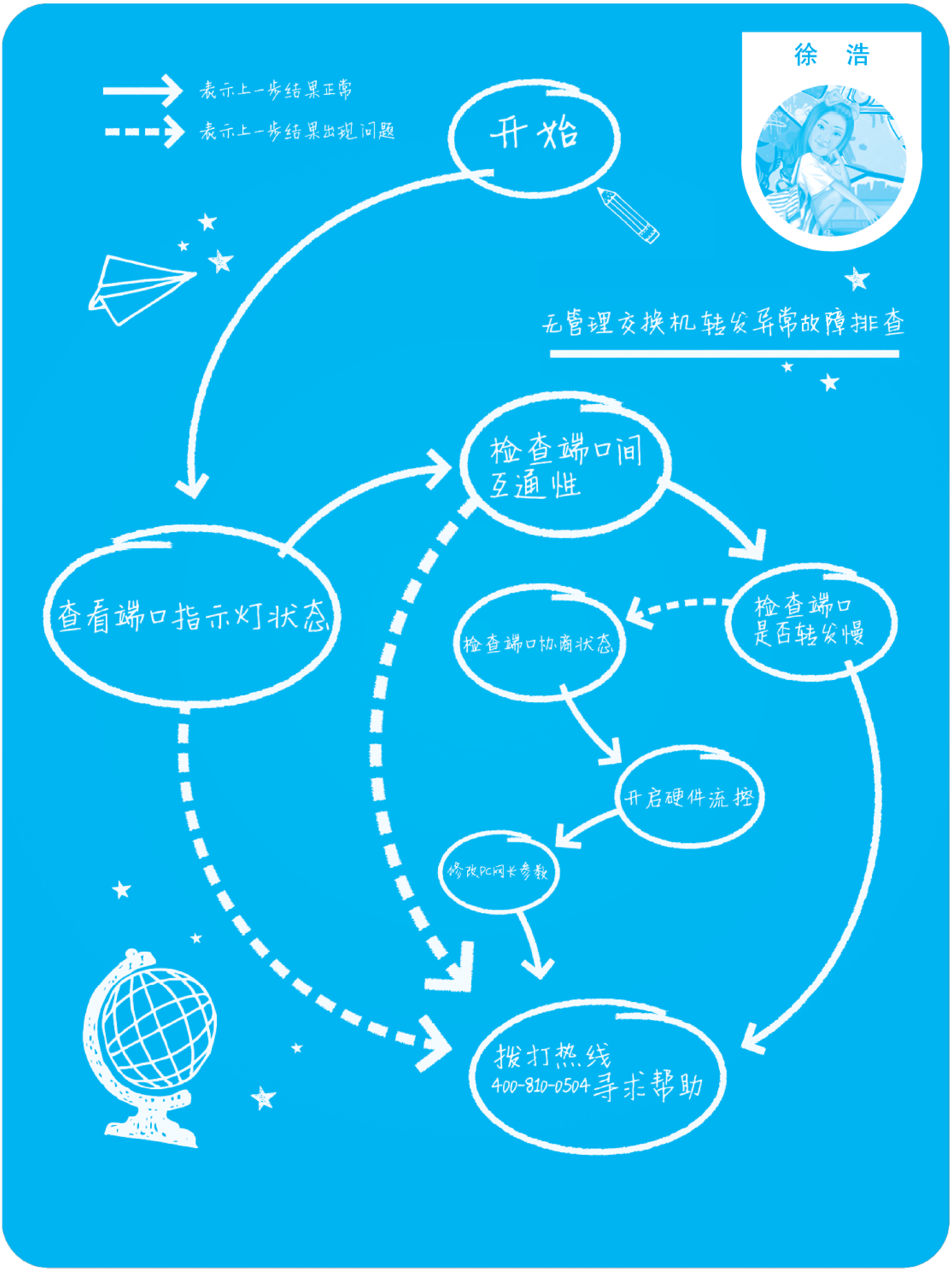
解决方法:尝试调整设备的负载分担类型。

```
link-aggregation load-sharing mode { destination-ip | destination-mac | destination-port | ingress-port |
source-ip | source-mac | source-port } *
```

(11) 抓包分析流量特点

如果试了各种负载分担类型还是分担不均,那么说明流量本身是不均匀的,建议抓包分析流量是现网流量自身特点导致的分担不均,如果本身某类流量就很多,hash 后该流量还是始终会 hash 到相同链路,所以这种情况下需要分析扩容是否可以对分担不均有改善。

如果流量模型没有某类流量大的情况,可直接收集设备信息再拨打热线 400-810-0504 寻求帮助。


徐 浩
表示上一步结果正常
表示上一步结果出现问题
开始
无管理交换机转发异常故障排查
检查端口间互通性
查看端口指示灯状态
检查端口是否转发慢
检查端口协商状态
开启硬件流控
修改PC网卡参数
拨打热线 400-810-0504 寻求帮助

1. 开始

SMB 无管理交换机涵盖：S1000 系列、S1200 系列、S132(4) S1324F。

定位故障的思路是：设备是否存在硬件故障，设备在网络中协商的端口状态是否正常，设备流控是否引起网络应用问题。

2. 流程图相关操作说明

(1) 查看端口指示灯状态

① 端口指示灯不插网线常亮，设备故障。

② 端口接网线，端口指示灯不亮，可重新插拔端口测试、更换网线测试、更换下连终端(如PC)测试，如果均无效果，设备故障。

③ 所有接网线的端口指示灯规律性快闪烁，查看是否存在环路，建议逐台插拔网线测试。

④ 所有接网线的端口指示灯同步交替闪烁，设备故障。

⑤ 所有接网线的端口指示灯只亮不闪，建议拔掉其他端口网线，单独测试端口互通性，取两台 PC 配置同网段地址互 ping，能否 ping 通(关闭防火墙等干扰设置)，若是不能 ping 通，设备故障。

(2) 检查端口间互通性

① 若无管理交换机端口之间不通，建议拔掉其他端口网线，单独测试端口互通性，取两台 PC 配置同网段地址，接在交换机连接 PC 的端口和连接上层设备的端口互 ping，观察是否能正常学习对端的 ARP 信息，能否 ping 通对端 IP 地址，若不能 ping 通，设备故障。

② 若上述两端口之间互通，但是和上层设备不通，建议排查上层设备故障。

(3) 检查端口是否转发慢

如果转发速率低于常规速率，建议继续排查端口问题。如果转发速率正常，建议求助呼叫中心。

一般性能的百兆网卡，传输(以 FTP 传输为例)速率如图 5-7 所示。

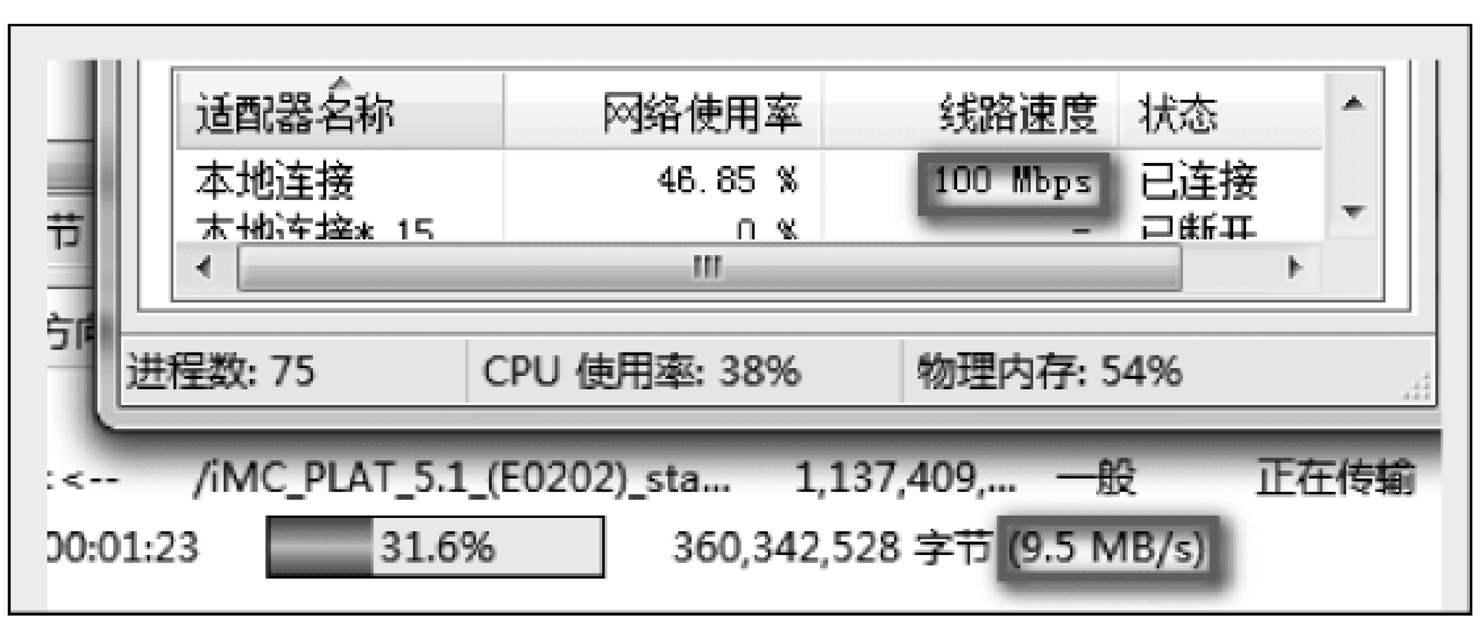


图 5-7 百兆网卡传输速率

一般性能的千兆网卡，传输(以 FTP 传输为例)速率如图 5-8 所示。

如果传输时，速率低于此平均值，建议排查传输慢问题。

(4) 检查端口协商状态

检查交换机端口指示灯是否工作在正确状态，如果显示状态有误，可尝试更换网线、更换端口测试，如更换端口解决，则设备故障。

无管理交换机端口指示灯常态如表 5-9 所示。

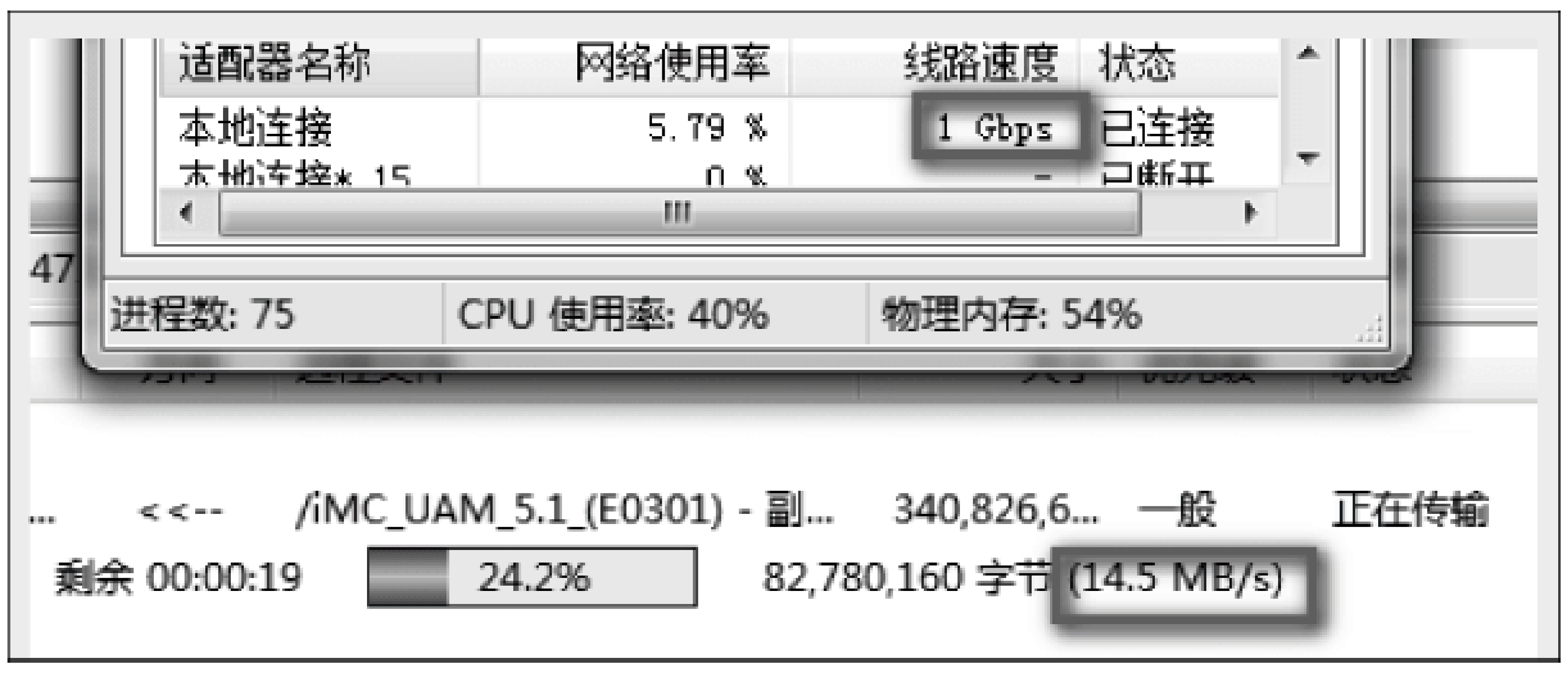


图 5-8　千兆网卡传输速率

表 5-9　无管理交换机端口指示灯常态

类　　型	端　　口	指　示　灯
全千兆交换机	Link/Act	绿灯：端口工作在 1000Mbps
		黄灯：端口工作在 10/100Mbps
		灭：以太网链路未建立
全千兆交换机	Link/Act	绿灯：以太网链路已建立
		绿灯闪烁：端口在收、发数据
		灭：以太网链路未建立
	Speed	绿灯：端口工作在 1000Mbps
		黄灯：端口工作在 10/100Mbps
		灭：以太网链路未建立
千兆上行交换机	Link/Act	绿灯：千兆端口工作在 1000Mbps 百兆端口工作在 10/100Mbps
		黄灯：千兆端口工作在 10/100Mbps
		灭：以太网链路未建立
千兆上行交换机	Link/Act	绿灯：以太网链路已建立
		绿灯闪烁：端口在收、发数据
		灭：以太网链路未建立
	Speed	绿灯：千兆端口工作在 1000Mbps 百兆端口工作在 10/100Mbps
		灭：千兆端口工作在 10/100Mbps 百兆端口工作在 10Mbps 以太网链路未建立
千兆上行交换机（含 combo 口）	Link/Act	绿灯：以太网链路已建立
		绿灯闪烁：端口在收、发数据
		灭：以太网链路未建立
	Speed	绿灯：千兆端口工作在 1000Mbps 百兆端口工作在 100Mbps 千兆 combo 口工作在 1000Mbps
		灭：千兆端口工作在 10/100Mbps 百兆端口工作在 10Mbps 千兆 combo 口 Down 以太网链路未建立
百兆交换机	Link/Act	绿灯：端口工作在 10/100Mbps
		灭：以太网链路未建立

(5) 开启硬件流控

将有硬件流控的设备流控开启(部分交换机存在可控的硬件流控;部分交换机固定流控关闭;部分交换机固定流控开启),将开关拨到"ON"时表明流控启用,拨到"OFF"时表明流控关闭,如图 5-9 所示。

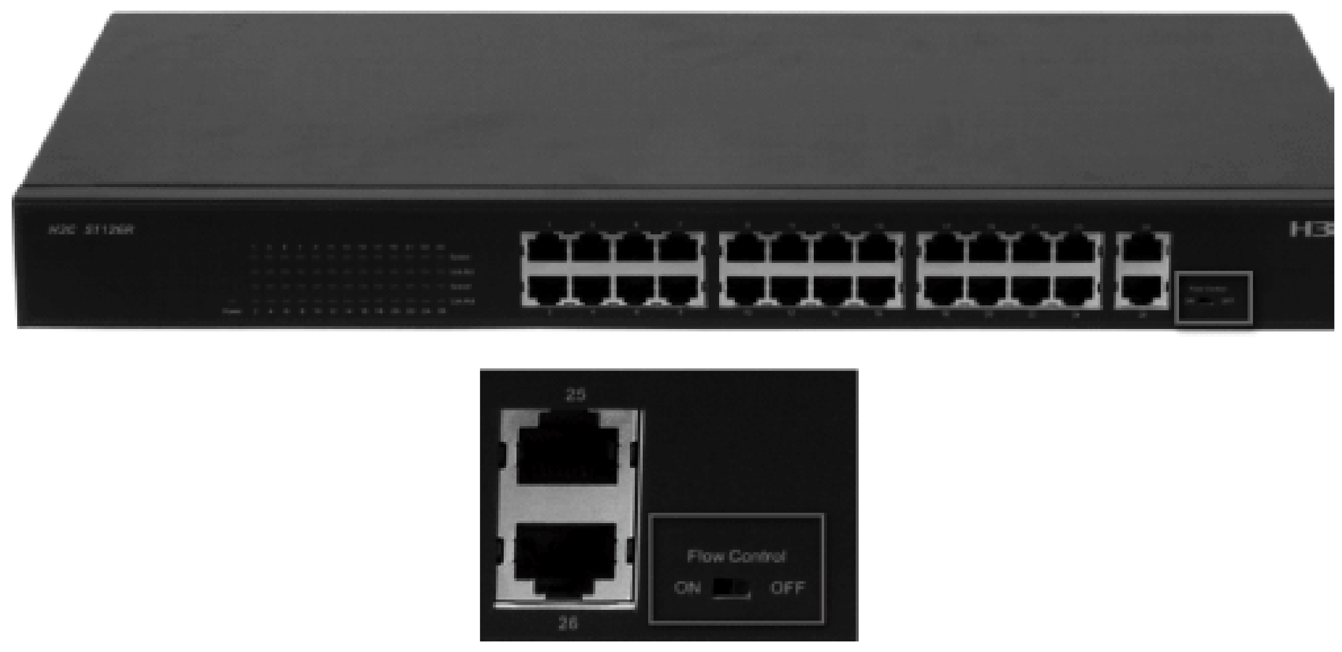


图 5-9 硬件流控开关

说明:改变流控开关状态后,需重启交换机使设置生效。

(6) 检查 PC 网卡参数

① 配合软件(如网络克隆软件、无盘操作系统、多媒体网络教学软件、文件同步传输软件)使用时,可将服务器的网卡强制成百兆全双工(一般服务器网卡使用都是千兆),网卡有流控设置项的也将流控开启。

② 在多媒体教学软件的使用中,还需要关闭传输网络中不工作的 PC 的远程唤醒功能,常见网卡的远程唤醒功能关闭方法如图 5-10 和图 5-11 所示。

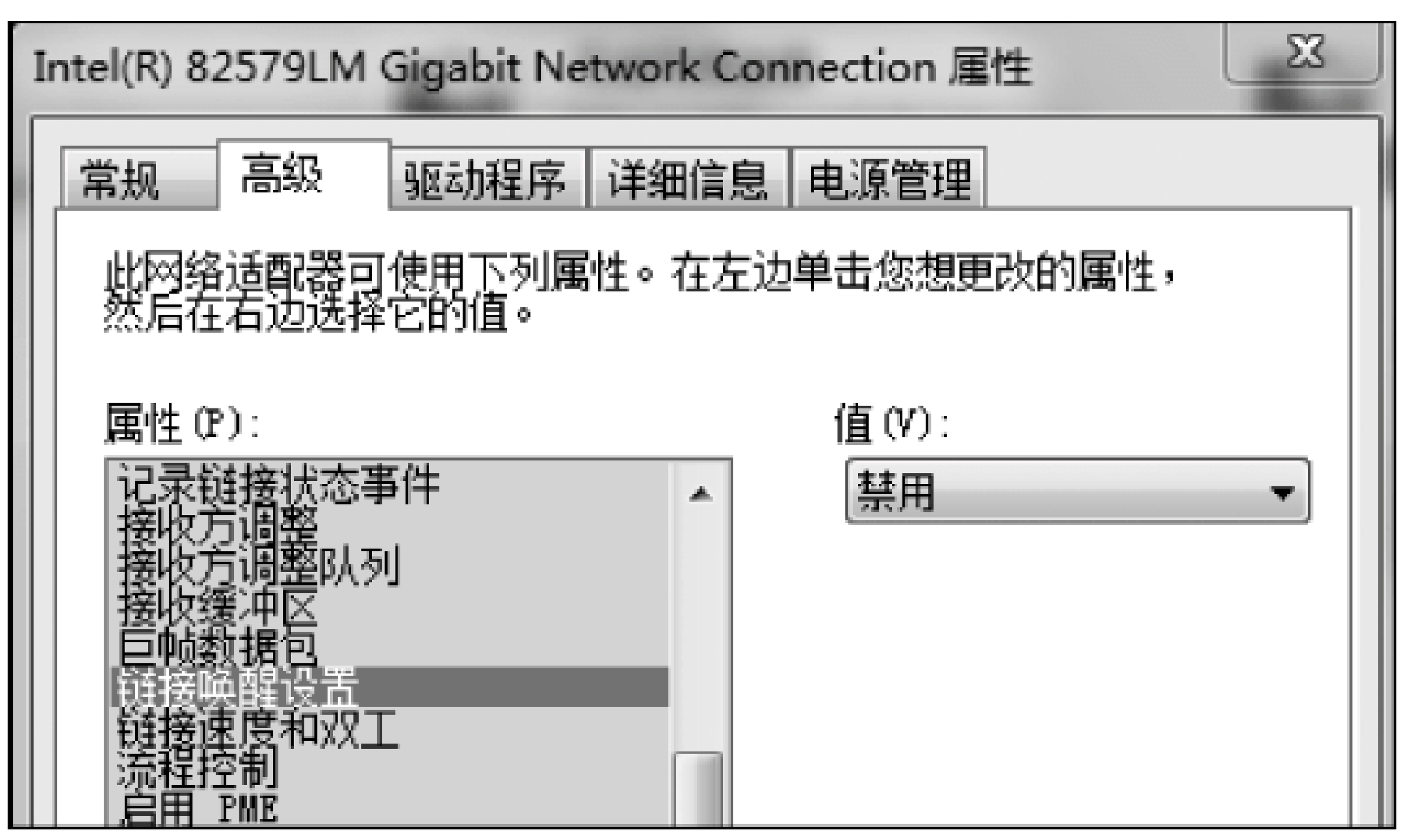


图 5-10 网卡型号是 Intel,远程唤醒方式设置

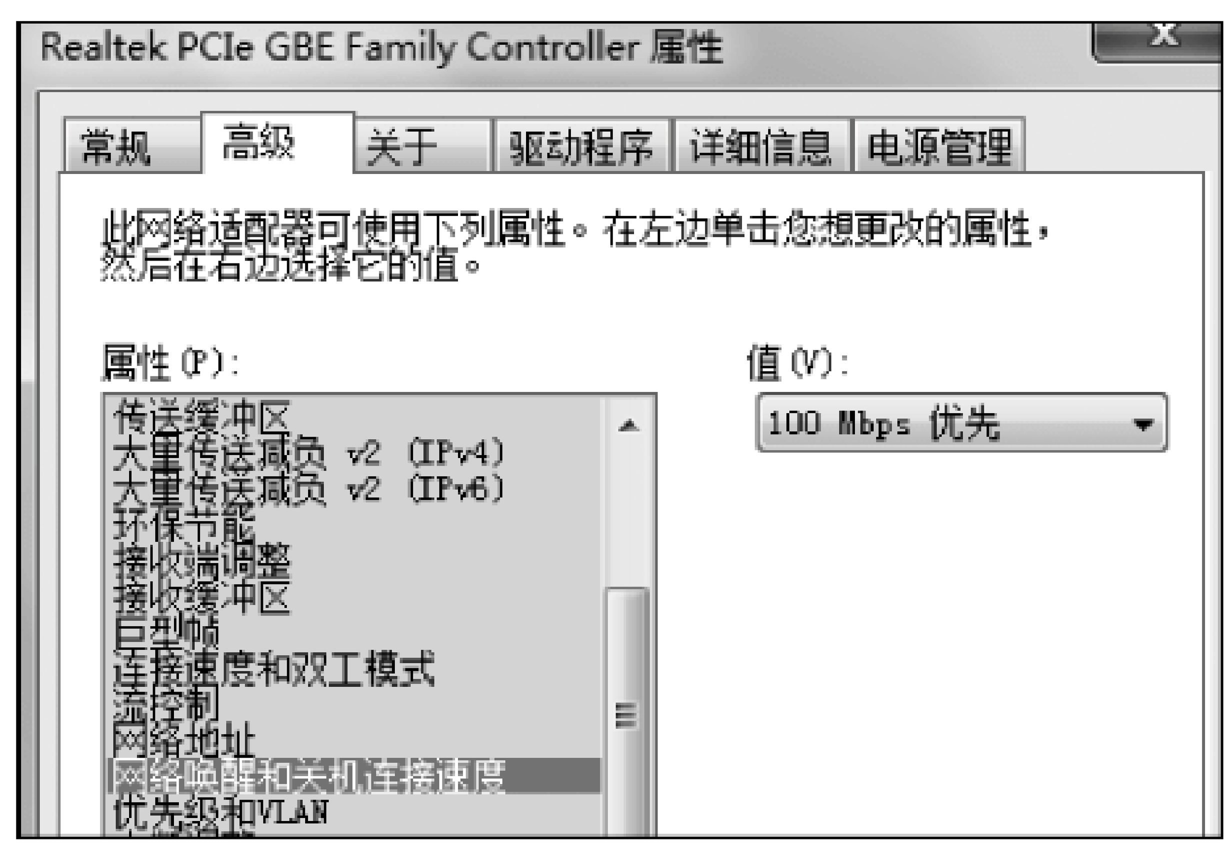
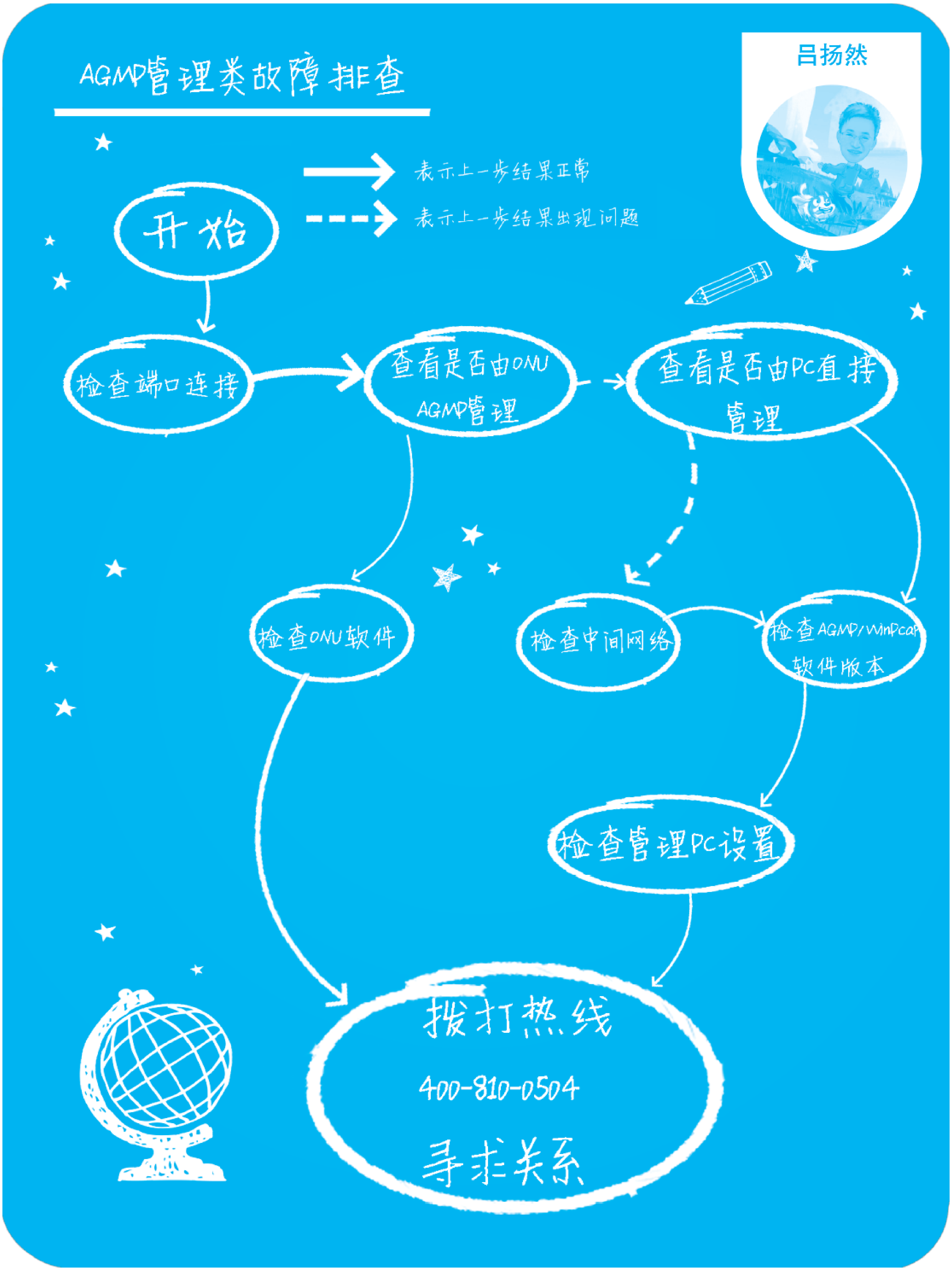


图 5-11 网卡型号是 Realtek,远程唤醒方式设置



AGMP管理类故障排查
吕扬然
表示上一步结果正常
表示上一步结果出现问题
开始
检查端口连接
查看是否由ONU AGMP管理
查看是否由PC直接管理
检查ONU软件
检查中间网络
检查AGMP/WinPcap软件版本
检查管理PC设置
拨打热线
400-810-0504
寻求关系

1. 开始

AGMP(Aolynk Group Management Protocol,Aolynk 组管理协议)是由 H3C 定义的基于链路层的局域网交换机管理协议。通过该协议可以远程管理局域网内的 H3C S1500E 系列楼道交换机。定位故障的思路是:先检查设备端口连接情况,再查看管理方式由 ONU 管理还是 PC 端 AGMP 软件管理,最后排查中间网络问题。

2. 流程图相关操作说明

(1) 检查端口连接

查看楼道交换机运行 AGMP 的端口是否连接正确。

S1516E/S1516E-AC60 使用 Uplink 口(端口 16)连接上层设备;S1524E 使用 Uplink 口(端口 24)连接上层设备。

运行 AGMP 协议的设备想管理下层 S1500E 系列交换机时,须与下层 S1500E 系列交换机的第一个端口或最后一个端口相连,且最后一个端口为上行口。

(2) 查看是否由 ONU AGMP 管理

ONU 的以太网口通过网线连接 S1500E 系列交换机的 Uplink 口,在 ONU 的 Web 设置页面上通过 AGMP 对交换机进行管理。

(3) 检查 ONU 软件版本

管理 S1500E 系列交换机的 ONU 建议升级软件至最新版本。

ONU 各软件版本 AGMP 相关问题列表如表 5-10 所示。

表 5-10 ONU 各软件版本 AGMP 相关问题

ONU 型号	软件版本	问题产生条件	问 题 现 象
ET716/ET724	102	同时用 ET716 和 AGMP 管理软件对 S1516E 交换机进行管理	S1516E 交换机出错
ET716/ET724	103	OLT 与 ET716/ET724 进行连接,ET716/ET724 下连接多台 S1516E/S1524E 交换机,管理 PC 与 OLT 相连接	无法使用 AGMP 管理软件对 S1516E/S1524E 交换机进行管理
ET716/ET724	103	ET716/ET724 连接指示灯位于端口右侧的 S1516E/S1524E 交换机	通过 ONU 无法管理交换机
ET254-L	103	进入网页执行 AGMP 管理 S1516E 操作	无法通过 AGMP 功能有效的管理 S1516E
ET254-L	105	使用硬件版本为“BC”的新 S1516E	通过 ONU 无法管理交换机
ET254-L	106	用 AGMP 管理软件和 ET254-L 同时管理 S1516E	在 AGMP 管理软件中修改端口模式为 Tagged,查看也是 Tagged,但是此时通过 ET254-L 读取的 VLAN 配置信息,端口模式仍然为 Transparent
ET254-L	111	ET254-L 连接指示灯位于端口右侧的 S1516E/S1524E 交换机	通过 ONU 无法管理交换机
ET254-L	117	使用 117 版本之前的 ET254-L 管理指示灯位于端口右侧的 S1516E/S1524E 交换机	指示灯位于端口右侧的 S1516E/S1524E 交换机 VLAN 混乱,数据转发不正确

更详细的问题列表，请查看对应设备最新的软件版本说明书。

(4) 查看是否由 PC 直连管理

管理 PC 通过网线连接 S1500E 系列交换机的 Uplink 口，运行 AGMP 管理软件对交换机进行管理。

(5) 检查 AGMP/WinPcap 软件版本

若当前管理设备的 AGMP 软件不是 R014 及以后版本，请联系呼叫中心获取最新的管理软件。

AGMP 管理软件是基于 WinPcap 运行，建议 WinPcap 软件为 3.0 或以上版本，若 WinPcap 软件版本过低可能会导致管理不到设备或其他异常情况。

(6) 检查管理 PC 设置

① 若本地管理 PC 上运行了相关安全软件，例如 Symantec 等杀毒软件，可能会影响 AGMP 管理软件的使用，在使用 AGMP 管理软件前，请先禁用此类软件，然后再对设备进行管理。

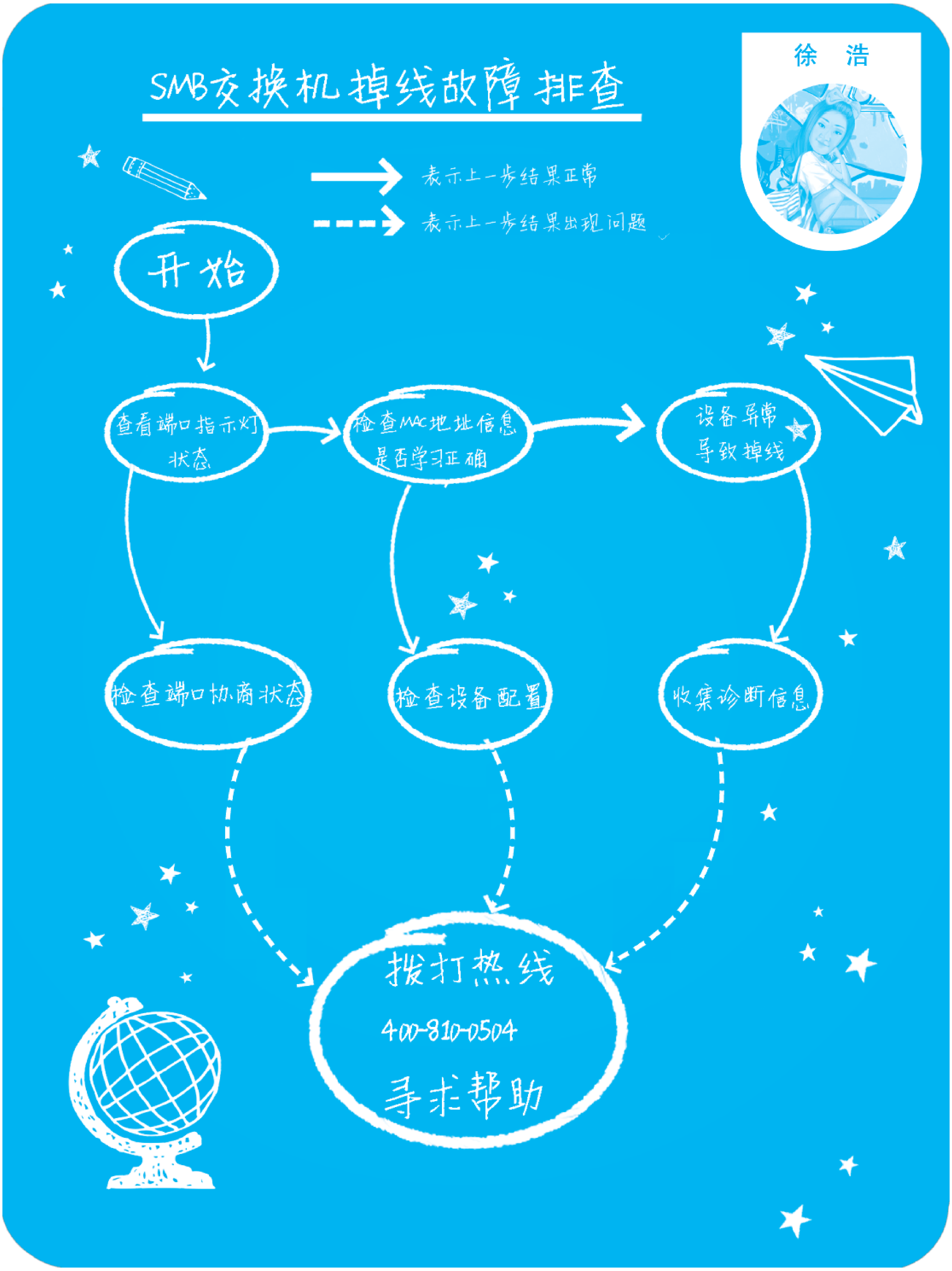
② 管理 PC 的差异性也可能会影响 AGMP 管理软件的使用，所以，在相同环境下可以尝试替换管理 PC 来判断是由于 PC 还是其他原因导致设备无法管理。

(7) 检查中间网络

① 检查 AGMP 管理报文经过的中间网络设备相关端口上是否已允许管理 VLAN 通过。若网络中存在指示灯位于端口左侧的 S1500E 系列交换机，请检查管理 PC 是否属于 VLAN 1319，并且中间网络设备相关端口上是否已允许 VLAN 1319 通过。

② 检查 AGMP 管理报文经过的中间网络设备相关端口上是否开启了广播风暴抑制功能，若开启，可尝试关闭该功能。

③ 检查当前所管理的设备是否处在一个大二层，建议通过划分管理 VLAN，将一个 VLAN 内的设备数量控制在 1000 以内，每个 VLAN 单独建立一个数据库文件进行管理。


SMB交换机掉线故障排查
徐　浩
表示上一步结果正常
表示上一步结果出现问题
开始
查看端口指示灯状态
检查MAC地址信息是否学习正确
设备异常导致掉线
检查端口协商状态
检查设备配置
收集诊断信息
拨打热线
400-810-0504
寻求帮助

1. 开始

SMB 交换机涵盖以下系列。

① 无管理交换机：S1000 系列交换机、S1200 系列交换机、S1300 系列交换机。

② 可管理交换机：S1500 系列交换机、S1600 系列交换机、S2100 系列交换机、S5000P 系列交换机、S5000E 系列交换机。

SMB 交换机一般做接入交换机，排查掉线的问题从单台设备入手。所以故障定位的思路是：先检查交换机的端口指示灯状态，再检查交换机是否学习到终端的 MAC 地址信息，最后判断是否设备异常导致的掉线。

2. 流程图相关操作说明

（1）查看端口指示灯状态

① SMB 交换机正常运行时，交换机的状态指示灯如表 5-11 所示。

表 5-11 交换机状态指示灯

<table>
<tr><th>类　型</th><th>端　口</th><th>指　示　灯</th></tr>
<tr><td rowspan="3">全千兆交换机</td><td rowspan="3">Link/Act</td><td>绿灯：端口工作在 1000Mbps</td></tr>
<tr><td>黄灯：端口工作在 10/100Mbps</td></tr>
<tr><td>灭：以太网链路未建立</td></tr>
<tr><td rowspan="6">全千兆交换机</td><td rowspan="3">Link/Act</td><td>绿灯：以太网链路已建立</td></tr>
<tr><td>绿灯闪烁：端口在收、发数据</td></tr>
<tr><td>灭：以太网链路未建立</td></tr>
<tr><td rowspan="3">Speed</td><td>绿灯：端口工作在 1000Mbps</td></tr>
<tr><td>黄灯：端口工作在 10/100Mbps</td></tr>
<tr><td>灭：以太网链路未建立</td></tr>
<tr><td rowspan="3">千兆上行交换机</td><td rowspan="3">Link/Act</td><td>绿灯：千兆端口工作在 1000Mbps
百兆端口工作在 10/100Mbps</td></tr>
<tr><td>黄灯：千兆端口工作在 10/100Mbps</td></tr>
<tr><td>灭：以太网链路未建立</td></tr>
<tr><td rowspan="5">千兆上行交换机</td><td rowspan="3">Link/Act</td><td>绿灯：以太网链路已建立</td></tr>
<tr><td>绿灯闪烁：端口在收、发数据</td></tr>
<tr><td>灭：以太网链路未建立</td></tr>
<tr><td rowspan="2">Speed</td><td>绿灯：千兆端口工作在 1000Mbps
百兆端口工作在 10/100Mbps</td></tr>
<tr><td>灭：千兆端口工作在 10/100Mbps
百兆端口工作在 10Mbps
以太网链路未建立</td></tr>
</table>

续表

类　　型	端　　口	指　示　灯
千兆上行交换机(含 combo 口)	Link/Act	绿灯：以太网链路已建立
		绿灯闪烁：端口在收、发数据
		灭：以太网链路未建立
	Speed	绿灯：千兆端口工作在 1000Mbps 百兆端口工作在 100Mbps 千兆 combo 口工作在 1000Mbps
		灭：千兆端口工作在 10/100Mbps 百兆端口工作在 10Mbps 千兆 combo 口 down 以太网链路未建立
百兆交换机	Link/Act	绿灯：端口工作在 10/100Mbps
		灭：以太网链路未建立
百兆交换机	Link/Act	绿灯：以太网链路已建立
		绿灯闪烁：端口在收、发数据
		灭：以太网链路未建立
	Speed	绿灯：端口工作在 100Mbps
		灭：端口工作在 10Mbps 或以太网链路未建立

② 掉线端口指示灯不插网线常亮，设备故障。

③ 掉线端口接网线，端口指示灯不亮，可重新插拔端口测试、更换网线测试、更换下连终端(如 PC)测试，如果均无效果，设备故障。

④ 掉线端口指示灯规律性快闪烁，查看是否存在环路，建议逐端口插拔网线测试或者开启 STP 功能，具体操作为页面向导：设备管理→STP 设置，STP 全局设置、端口设置分别如图 5-12 和图 5-13 所示。



图 5-12　STP 全局设置



图 5-13　STP 端口设置

⑤ 掉线端口指示灯只亮不闪，建议拔掉其他端口网线，单独测试端口互通性，取两台 PC 配置同网段地址互 ping，能否 ping 通（需关闭防火墙等设置），若是不能 ping 通，设备故障；

（2）检查端口协商状态

检查端口协商的状态是否正确（针对可管理的交换机排查）。可通过查看 Web 界面来确认端口的协商速率和双工信息。如果协商异常，建议更换网线、PC、端口。

Web 查看如图 5-14 所示，具体操作为页面向导：端口管理→端口设置→端口设置。



图 5-14　端口设置

（3）检查 MAC 地址信息是否学习正确

① 无管理交换机排查：在 PC 端查看是否学到对端 PC 的 ARP 信息，如果学习到 ARP 信息，但是 ping 不通对端 PC 地址，建议在两边的 PC 上同时抓包查看；如果学不到 ARP 信息，建议在无管理交换机上换端口测试或替换交换机测试。

② 可管理交换机排查：在可网管的交换机上是否学到正确的 MAC 地址信息，可以通过 Web 界面查看。Web 查看如图 5-15 所示，具体操作为页面向导：设备管理→MAC 设置→MAC 显示。

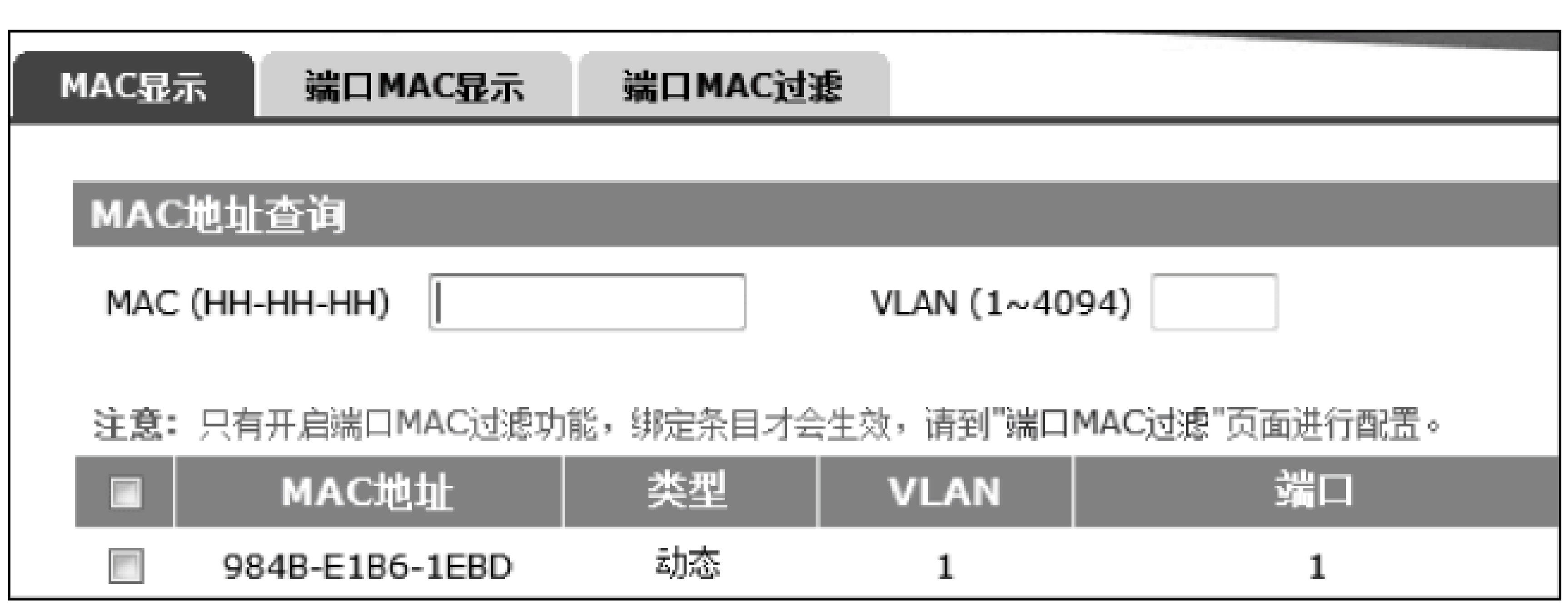


图 5-15　MAC 显示

(4) 检查设备配置

无管理交换机不可配置,以下检查可管理交换机的配置。

如果在交换机上没有学到终端的MAC地址信息,可检查是否以下配置导致。

① 是否配置了端口过滤,如果该端口开启MAC过滤功能,那么只有符合该端口绑定条件的终端MAC可以通过,未绑定终端MAC无法通过该端口。

Web查看如图5-16所示,具体操作为页面向导:设备管理→MAC设置→端口MAC过滤。



图5-16 端口MAC过滤

② 是否配置基于端口的VLAN导致与其他端口隔离。SMB交换机的VLAN配置包含802.1Q VLAN和基于端口的VLAN两种,两种VLAN模式互斥(H3C S1526交换机——端口指示灯在面板右边的例外,它支持两种VLAN共同使用)。如果端口配置了端口组VLAN且此端口只属于这个VLAN,那么该端口与其他不属于此端口组的端口二层隔离,不能互通,但是交换机可以学到此端口上来的MAC。

Web查看基于端口的VLAN配置如图5-17所示,具体操作为页面向导:设备管理→VLAN设置→基于端口VLAN。

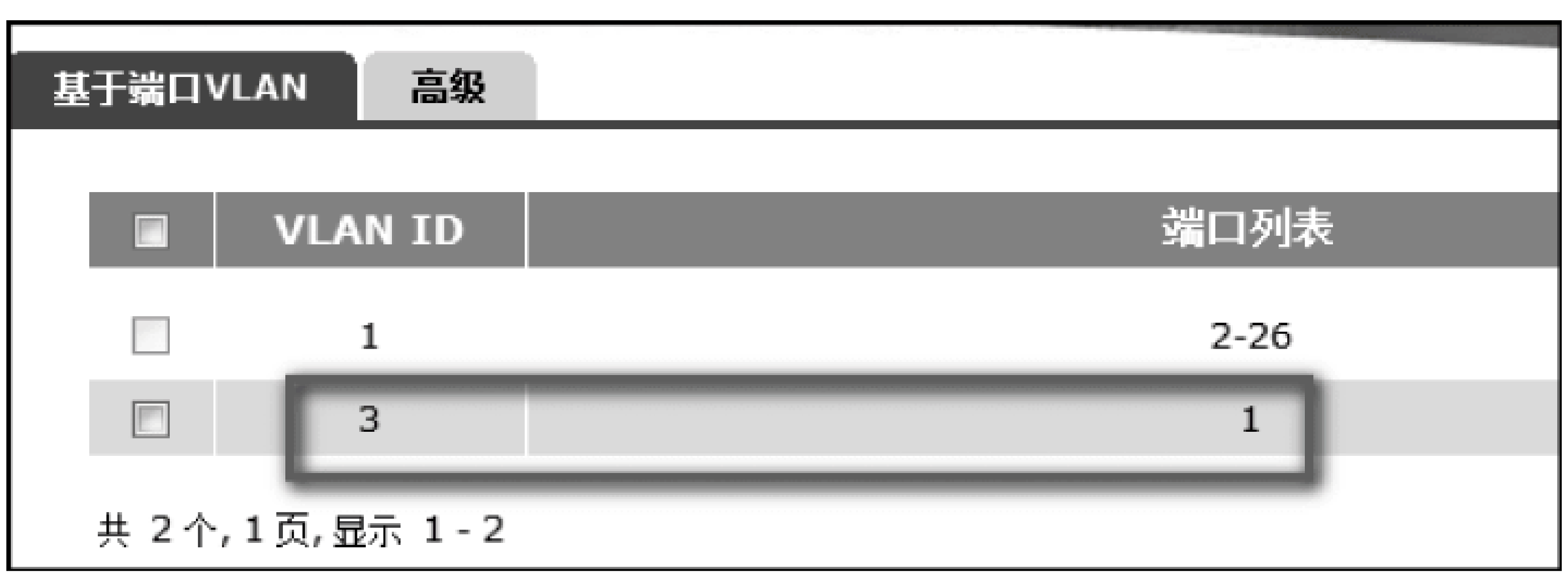


图5-17 基于端口VLAN

(5) 设备异常导致掉线

① 无管理交换机可以采用替换掉线端口或替换设备解决,如果替换掉线端口或替换设备可以解决,则属于设备异常。

② 可管理交换机可尝试查看端口的统计报文,看端口的收发数据包是否正常,统计的报文类型是否有异常,在Web界面上查看如图5-18所示,具体操作为页面向导:端口管理→端口设置→端口统计。

③ 端口的接收报文描述如表5-12所示。



图 5-18　端口统计

表 5-12　端口接收报文描述

接 收 统 计	描　　述
总数据包	接收报文的总数量
总字节数	接收报文的总字节数
广播包	接收广播报文的总数量
多播包	接收多播报文的总数量
接收错误包	接收错误报文的总数量
Runts 错误包	CRC 正确，且数据帧长度小于 64 字节的报文数量
Giants 错误包	CRC 正确，且数据帧长度大于 1518 字节的报文数量
CRC 错误包	CRC 错误，且数据帧长度处于 64～1518 字节的报文数量
Frame 错误包	数据帧长度处于 64～1518 字节，且报文的 FCS(帧校验序列)的字节数为非整数的报文数量
Aborts 错误包	接收到的非法报文总数，非法报文包括： 报文碎片：长度小于 64 字节(长度可以为整数或非整数)且 CRC 校验错误的帧； jabber 帧：大于 1518 或 1522 字节，且 CRC 校验错误(报文字节可以为整数或非整数)； 符号错误帧：报文中至少包含 1 个错误的符号； 长度错误帧：报文中 802.3 长度字段与报文实际长度(46～1500 字节)不匹配
Ignored 错误包	由于端口接收缓冲区不足等原因而丢弃的报文数量

④ 端口发送报文描述如表 5-13 所示。

表 5-13　端口发送报文描述

发 送 统 计	描　　述
总数据包	发送报文的总数量
总字节数	发送报文的总字节数
广播包	发送广播报文的总数量
多播包	发送多播报文的总数量
发送错误包	发送错误报文的总数量

续表

发送统计	描　述
Aborts 错误包	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
Deferred 错误包	第一次传输请求由于网络忙而延迟的报文数量
Collisions 错误包	端口在报文传输过程中所产生冲突的报文数量
Late collisions 错误包	延迟冲突帧的数量，延迟冲突帧是指帧的前 512b 已经被发送，由于检测到冲突，该帧被延迟发送

（6）收集诊断信息

收集一键导出信息收集需要在 Web 界面上操作，具体位置如图 5-19 所示。

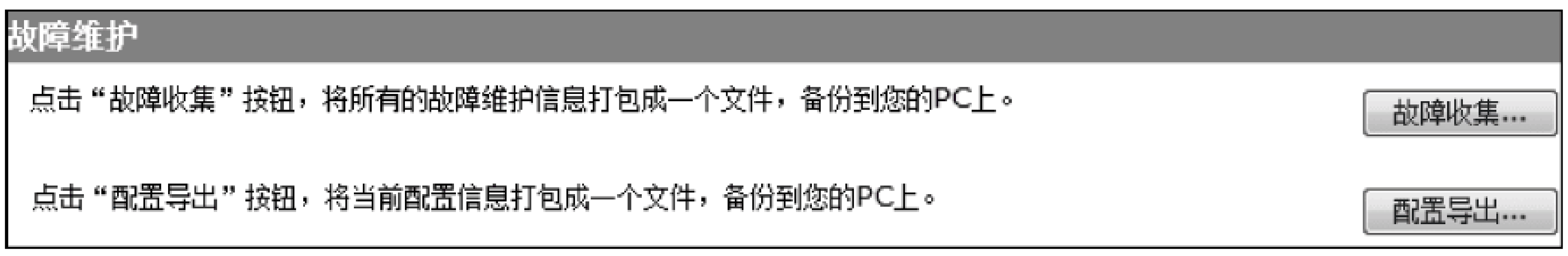
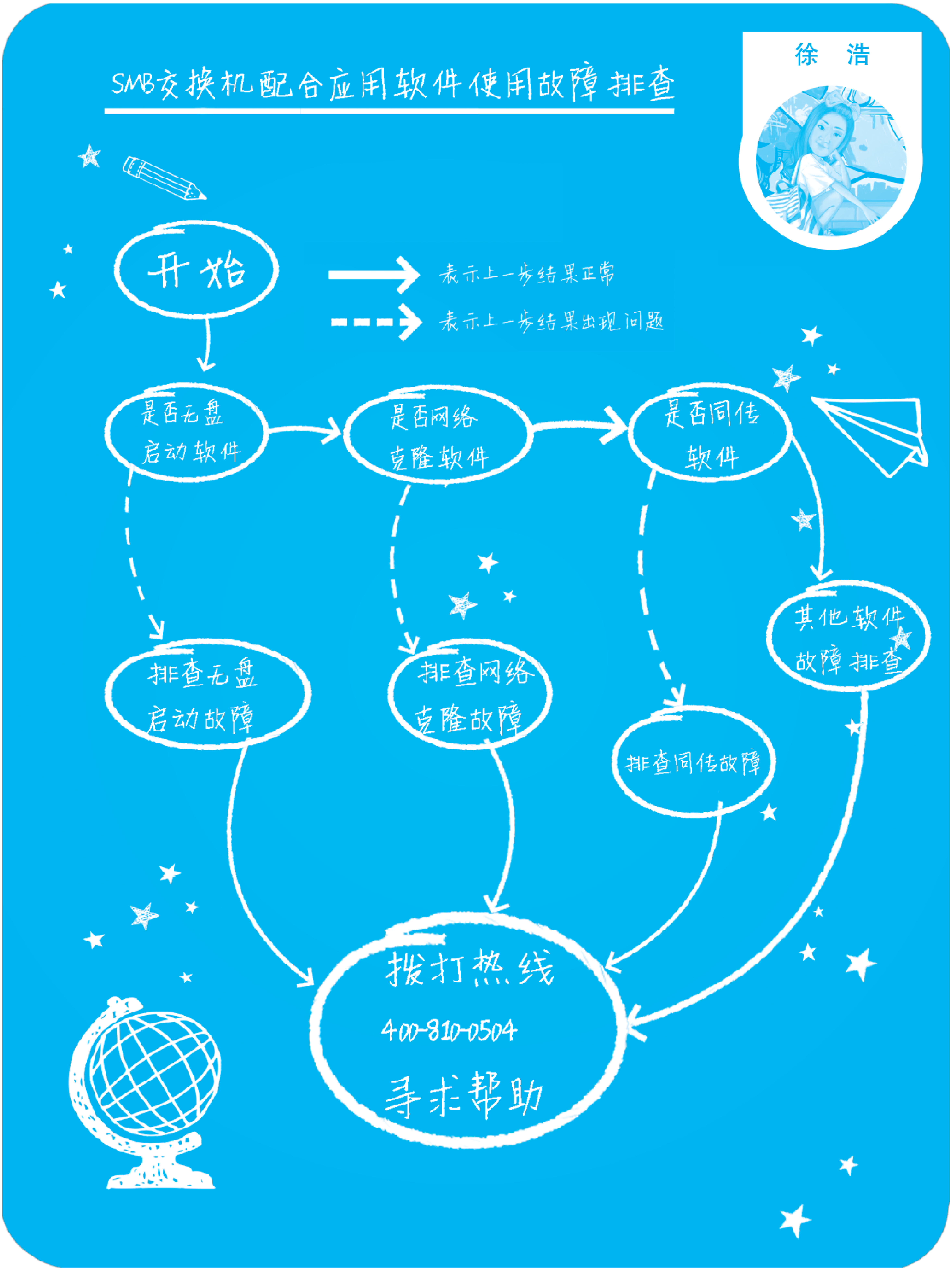


图 5-19　故障维护

将以上信息收集整理，并详细了解故障现象和现场网络拓扑，求助呼叫中心处理。


徐 浩
SMB交换机配合应用软件使用故障排查
开始
表示上一步结果正常
表示上一步结果出现问题
是否无盘启动软件
是否网络克隆软件
是否同传软件
排查无盘启动故障
排查网络克隆故障
排查同传故障
其他软件故障排查
拨打热线
400-810-0504
寻求帮助

1. 开始

SMB 交换机涵盖以下系列。

① 无管理交换机：S1000 系列交换机、S1200 系列交换机、S1300 系列交换机。

② 可管理交换机：S1500 系列交换机、S1600 系列交换机、S2100 系列交换机、S5000P 系列交换机、S5000E 系列交换机。

SMB 交换机配合应用软件使用时，需要根据客户的网络拓扑来排查，所以配合应用软件定位的故障的思路：根据不同类型的应用软件，从网络拓扑入手排查。

2. 流程图相关操作说明

(1) 是否无盘启动软件

检查 PC 客户端是否是无盘电脑，是否为无盘无法启动或无盘启动慢问题。

(2) 排查无盘启动故障

无盘启动软件配合交换机使用时，一般出现的问题是无盘客户端无法启动、启动慢，网络故障排查方法如下。

① 无盘启动环境建议采用全千兆网络设备进行组网，PC 和服务器端网卡均采用千兆自协商模式。

② 检查网络拓扑。是否存在百兆、千兆客户端混接情况。如果客户端为百兆，服务器为千兆，交换机必须支持并打开流控。

③ 在千兆、百兆混接的拓扑中，如果交换机默认流控关闭且不支持设置，可以尝试将服务器强制成百兆全双工尝试。

④ 如果在无盘启动 PXE(Preboot Execution Environment，远程引导技术)阶段出现故障，可能是客户端 PXE 驱动异常，建议刷新网卡 PXE 程序和主板 BIOS 到最新版本。

(3) 是否网络克隆软件

检查 PC 客户端是否为使用网络克隆软件慢问题。

(4) 排查网络克隆故障

网络克隆软件配合交换机使用时，一般出现的问题是网克慢，网络故障排查方法如下。

① 建议使用单台交换机分批对客户端进行网克，减少网克客户端的数量，且尝试将服务器网克的端口和别的业务端口划分 VLAN 区分。

② 如果网络中的交换机端口(包括服务器的端口和接入交换机的端口)开启了流控，建议将流控关闭。

③ 如果端口开启了广播风暴抑制，建议将广播风暴抑制关闭。

④ 如果在网络克隆过程中出现个别端口协商异常(协商成低速端口)，拔掉协商异常的端口网线。

⑤ 如果上述步骤实施后网克问题没有解决，则尝试升级网卡的 BIOS 程序到最新版本或者更新 MAXDOS 程序版本。

(5) 是否同传软件

检查 PC 客户端是否为使用同传软件慢问题。

(6) 排查同传故障

同传软件在配合交换机使用时,一般出现的问题是同传慢,排查网络故障方法如下。

① 需要同传的PC需将服务器的网卡强制成百兆全双工(一般服务器网卡使用都是千兆),网卡有流控设置项的也将流控开启。

② 在同传软件的多媒体教学使用中,还需要关闭传输网络中不工作的PC的远程唤醒功能,常见网卡的远程唤醒功能关闭方法如图5-20～图5-22所示。

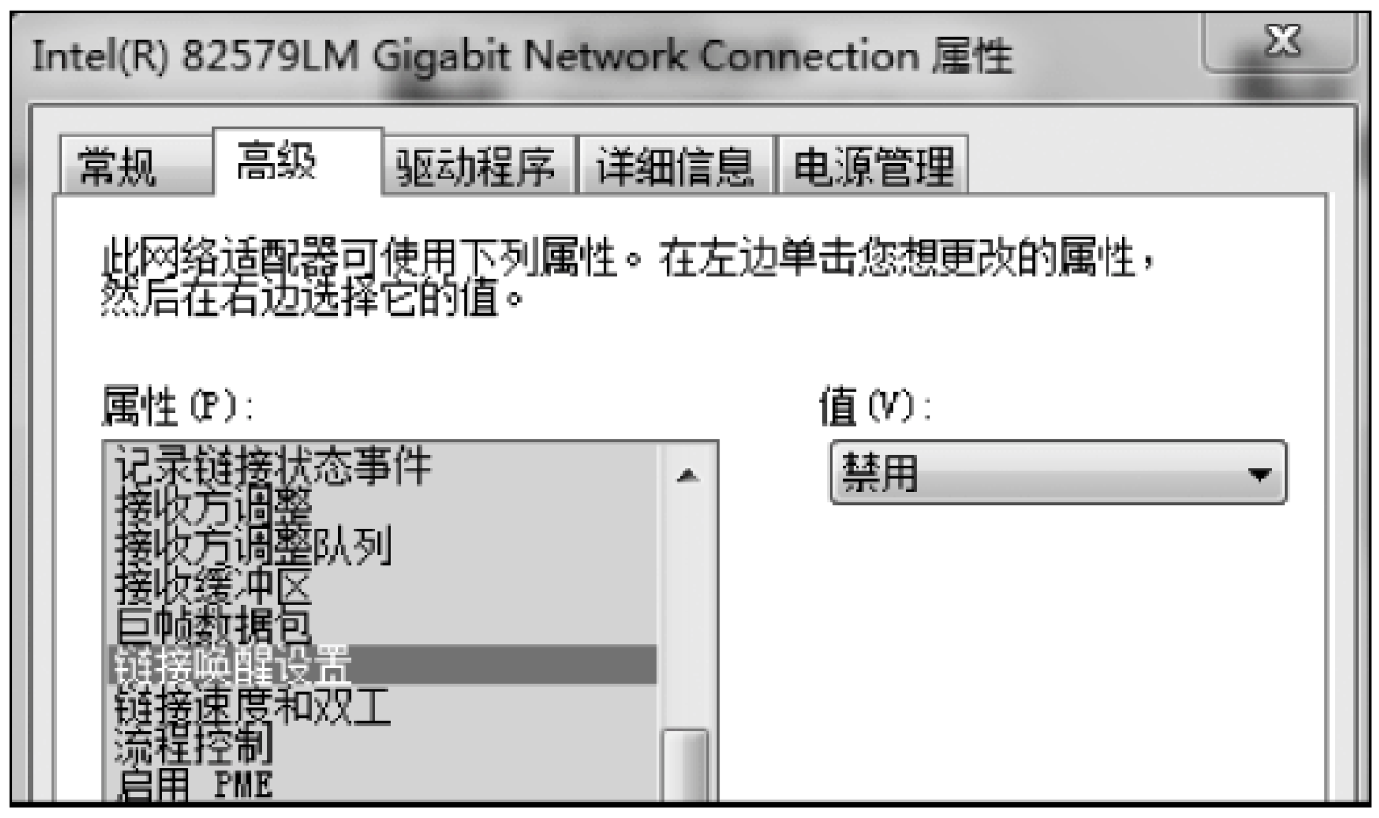


图5-20 网卡型号是Intel,远程唤醒方式设置



图5-21 网卡型号是Realtek,远程唤醒方式设置

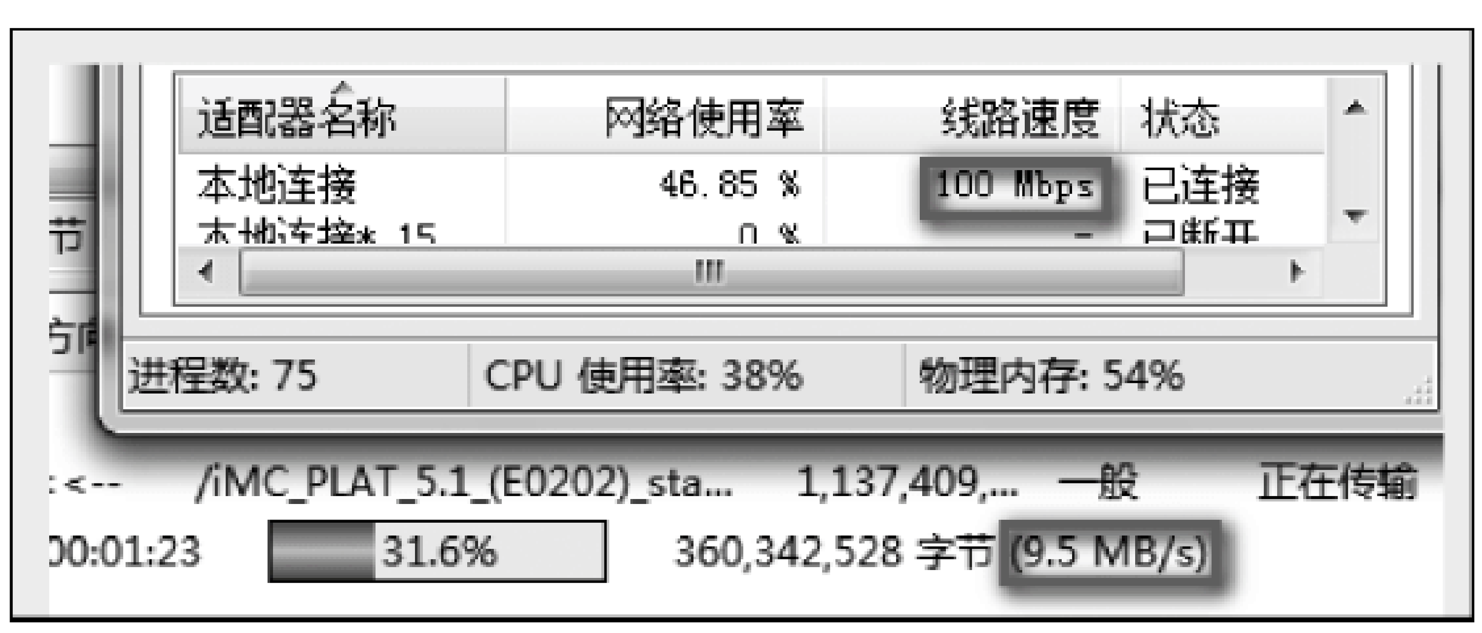


图5-22 百兆全双工传输速率

一般性能的千兆网卡,传输(以FTP传输为例)速率如图5-23所示。

如果传输时,速率低于此平均值,建议排查同传慢问题。

(7) 其他软件故障排查

配合其他软件使用,例如KTV点歌软件,英保通软件等,基本的排查思路如下。

① 检查网络拓扑,是否存在服务器、客户端的千兆、百兆混接情况,排除网络拥塞。

② 应用软件的传输方式如果是广播方式(包括组播和未知单播),部分SMB交换机存在

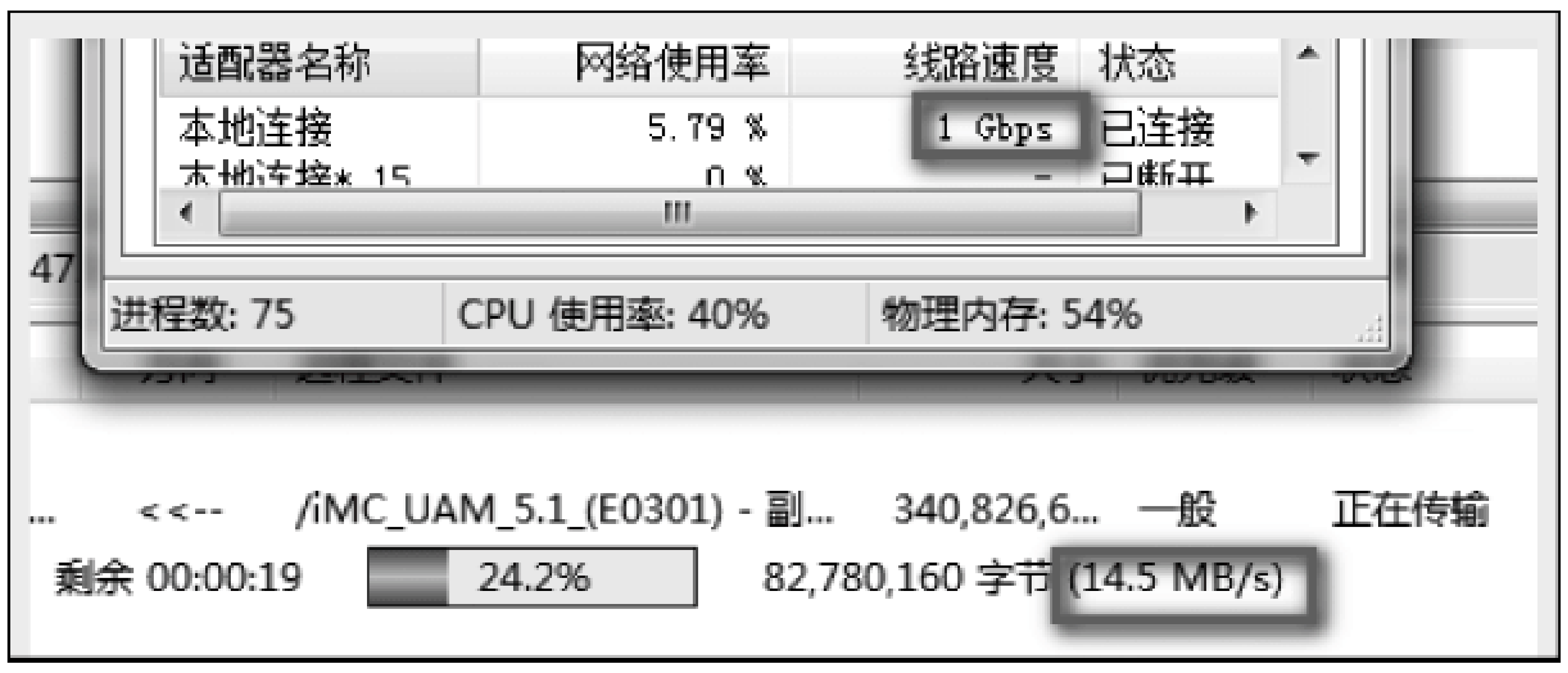
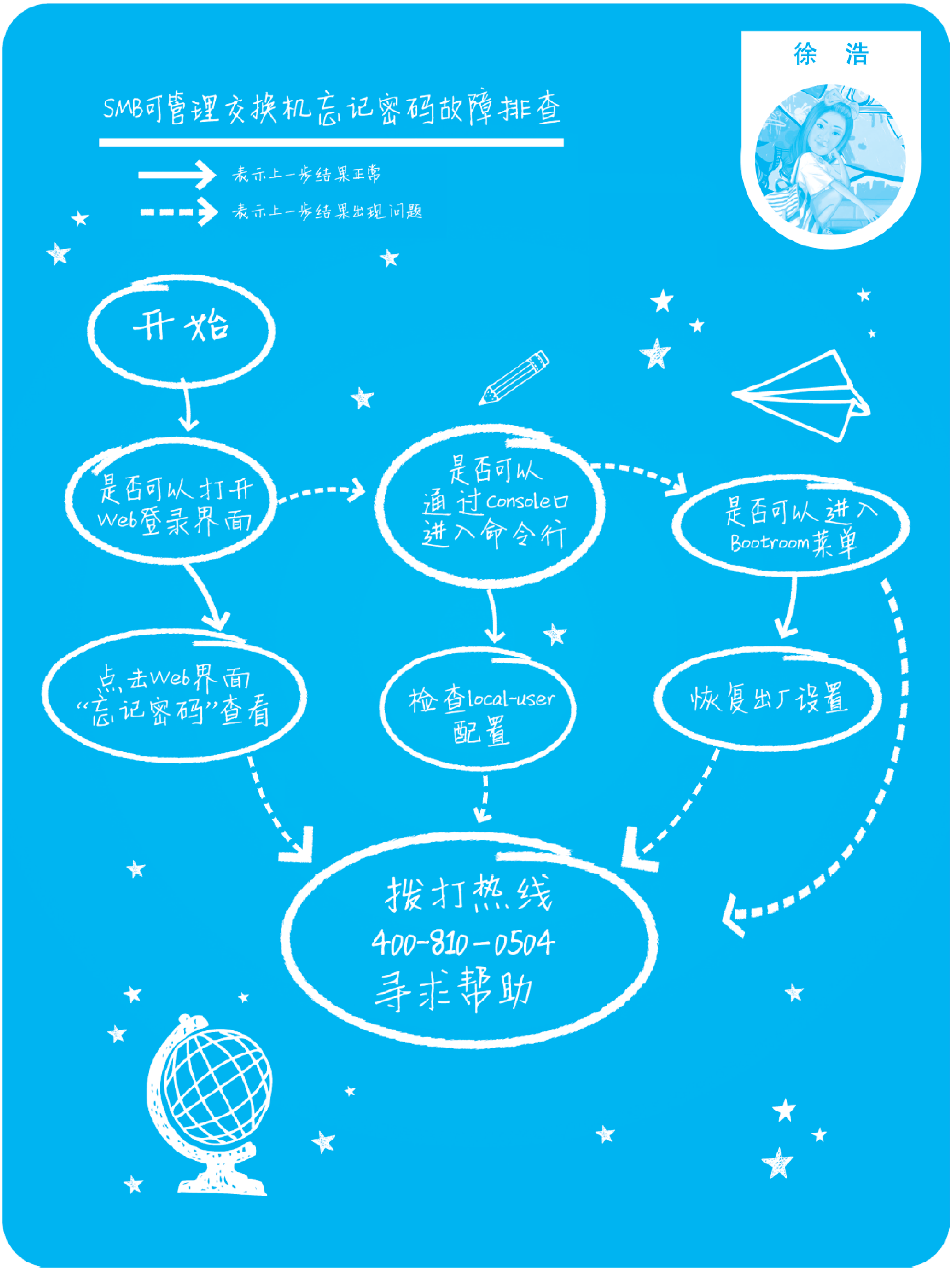


图 5-23　千兆网卡传输速率

广播报文转发入口抑制的问题，即广播报文只能按照最低速率端口的接受能力进行转发，所以需要排除网路中的低速端口。

③ 如果以上措施无法解决，建议收集现场网络拓扑，使用的应用软件版本、型号，使用的网卡信息、驱动版本，联系呼叫中心处理。


徐 浩
SMB可管理交换机忘记密码故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
是否可以打开Web登录界面
是否可以通过console口进入命令行
是否可以进入Bootroom菜单
点击Web界面“忘记密码”查看
检查local-user配置
恢复出厂设置
拨打热线
400-810-0504
寻求帮助

1. 开始

SMB 可管理交换机涵盖以下系列：S1500 系列交换机、S1600 系列交换机、S2100 系列交换机、S5000P 系列交换机、S5000E 系列交换机。

忘记密码问题的解决思路是：先检查是否可以登录 Web 界面解决，再检查是否可以通过 Console 口进入交换机命令行解决，最后检查是否可以进入交换机的 Bootroom 界面解决。

2. 流程图相关操作说明

(1) 是否可以打开 Web 登录界面

检查是否可以打开交换机的登录界面，SMB 可管理交换机默认的管理地址为 192.168.0.233(S5000P 系列、S5000E 系列)或者 192.168.0.234(S1500 系列、S1600 系列、S2100 系列)。

(2) 单击 Web 界面"忘记密码"按钮查看

如果输入管理地址可以打开 Web 界面，但是忘记用户名或者密码的，可以单击如图 5-24 所示的"忘记密码"按钮。



图 5-24 Web 界面

单击之后会弹出处理忘记密码的详细步骤，按照步骤操作即可，操作如图 5-25 所示。

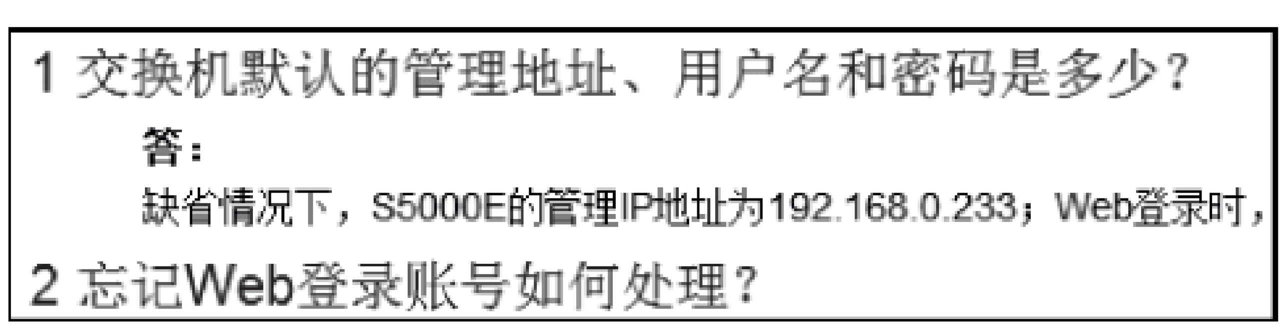


图 5-25 忘记密码操作

(3) 是否可以通过 Console 口进入命令行

如果无法登录到交换机的 Web 登录界面，则确认是否可以通过 Console 口进入设备的命令行。

(4) 检查 local-user 配置

进入设备系统视图后，建议用户查看当前用户，并根据用户类型来重置密码。

命令：*display local-user*

例如：通过命令行查看当前设备上的用户和详细信息，查看信息如下。

```
[H3C]display local-user
1   The contents of local user admin:
    State               :Active
    ServiceType Mask    :W
    Level               :1

2   The contents of local user telnet:
    State               :Active
    ServiceType Mask    :T
    Level               :1

3   The contents of local user ftp:
    State               :Active
    ServiceType Mask    :C
    Level               :1

Total 3 local user(s) matched.
ServiceType Mask Meaning: C--Terminal   T--Telnet   W--Web
```

通过查看到的用户名，进入相应视图重置密码。

命令：*password simple 123*

例如：通过命令行重置 telnet 的密码，设置信息如下。

```
[H3C]local-user telnet
[H3C-luser-telnet] password simple 123
```

说明：老款 S1526(指示灯位于端口左侧)交换机如果忘记密码，只能通过命令行的恢复出厂设置解决，无法通过重置用户类型密码处理。

(5) 是否可以进入 Bootroom 菜单

如果用户设置了 Console 口密码且遗忘，则无法进入命令行设置。

```
****************************************************************************
*       Copyright (c) 2010-2013 Hangzhou H3C Technologies Co., Ltd.        *
*       All rights Reserved.                                               *
*       Without the owner's prior written consent,                         *
*       no decompiling or reverse-engineering shall be allowed.            *
****************************************************************************

User interface Aux0/0 is available

Please press ENTER.


Login authentication

Password:
```

这时需要用户重启设备，进入 Bootroom 界面设置，默认进 Bootroom 的密码为空。如果用户设置了 Bootroom 密码且密码忘记，则无法执行此操作，建议联系呼叫中心处理。

(6) 恢复出厂设置

进入 Bootroom 界面之后，显示菜单如下。

```
Press Ctrl-B to enter Boot Menu...3
Password:

                    BOOT MENU
          1. Download application file to flash
          2. Modify bootrom password
          3. Restore default configurations of applicaiton
          0. Reboot system

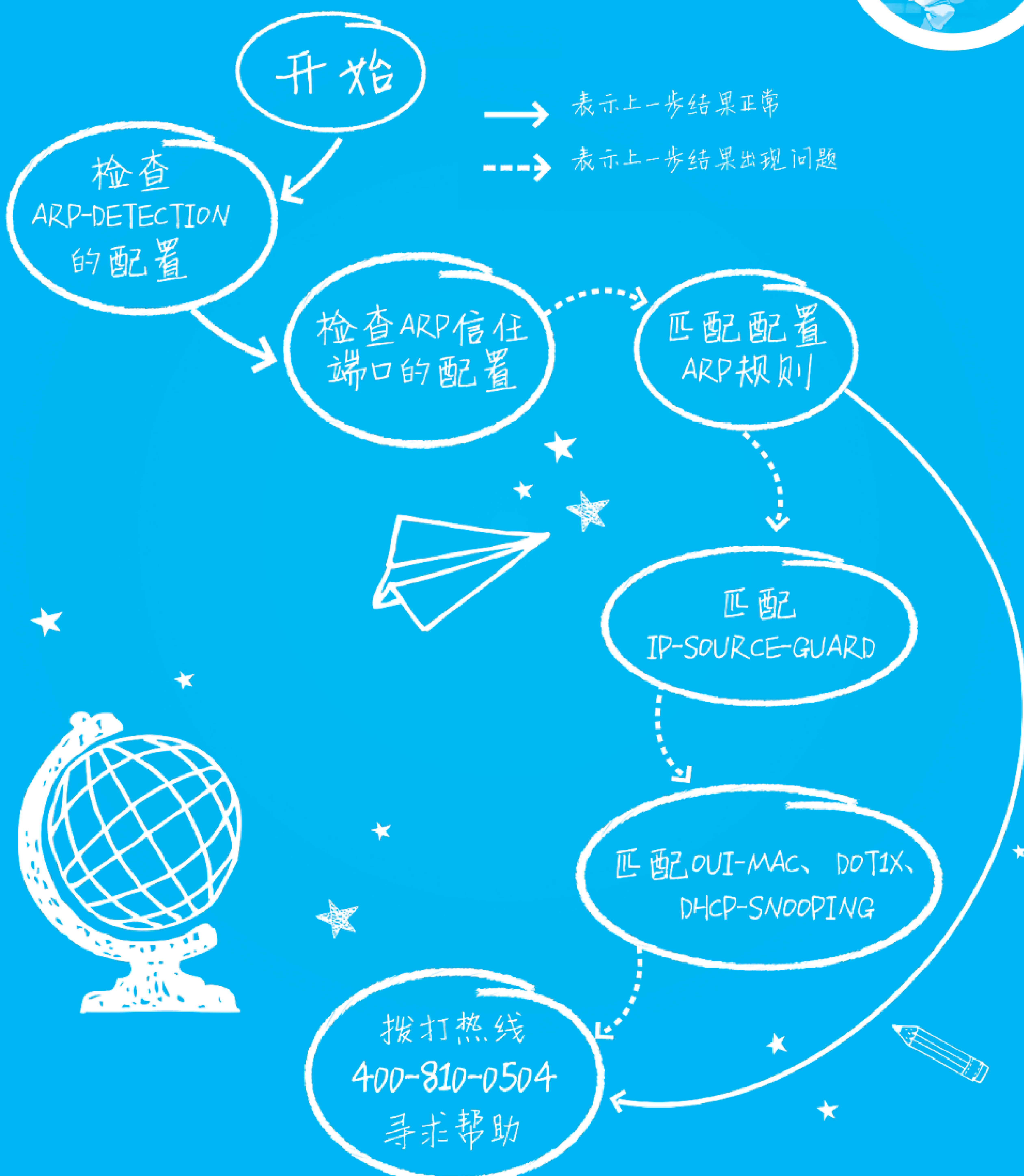
Enter your choice(0-3):3
```

选择 3 号菜单,执行“恢复出厂设置”命令。在配置恢复出厂以后,可以选择 0 号菜单执行重启操作,重新登录设备即可使用。

ARP-DETECTION故障排查

彭绍穗





1. 开始

定位故障思路是：开始先检查 ARP-DETECTION 是否正确使能。如果配置无问题，再看目的端口是否为 ARP 信任端口。如果不是 ARP 信任端口，则需要进行用户的合法性检查。关于用户合法性检查，首先进行的是匹配 ARP 规则，如果匹配，则按照规则处理，如果不匹配，则查看是否匹配 IP SOURCE GUARD。关于 IP-SOURCE-GUARD 的匹配，如果找到对应的 IP 表项，则判断是否非法，如果不匹配，则查看是否匹配 OUI-MAC、DOT1X、DHCP-SNOOPING 的其中一项。

2. 流程图相关操作说明

(1) 检查 ARP-DETECTION 的配置

查看 ARP-DETECTION 在设备上对应的 VLAN 中是否使能。如果未使能，则进行下一步处理。

命令：*display arp detection*

例如：ARP-DETECTION 在 VLAN 10 中使能，则有如下显示。

```
[H3C]dis arp detection
 ARP detection is enabled in the following VLANs:
 1,10
```

(2) 检查 ARP 信任端口的配置

查看该 ARP 所在或所应该的端口是否为信任端口，如果不为信任端口，则进行下一步处理。

命令：*display this*

例如：Ten-GigabitEthernet 5/0/1 为 ARP 信任端口。

```
[H3C-Ten-GigabitEthernet5/0/1]display this
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 1 untagged
arp detection trust
```

(3) 匹配配置规则

查看在设备上是否配置了 ARP 的规则。如果匹配，则按照规则处理(permit/deny)，如果未匹配，则进行下一步处理。

命令：*display arp detection*

例如：IP 为 1.1.1.0/24，MAC 为 2222-2222-2200/ffff-ffff-ff00 的 ARP，被丢弃。

```
[H3C]display arp detection
 ARP detection is enabled in the following VLANs:
 1, 10

 ARP detection:
 arp detection 0deny ip 1.1.1.0 255.255.255.0 mac 2222-2222-2200 ffff-ffff-ff00
```

（4）匹配 IP-SOURCE-GUARD

查看是否匹配 IP SOURCE GUARD 的静态配置。如果找到了对应源 IP 地址的静态绑定表项但源 MAC 地址不符，认为该 ARP 报文非法，进行丢弃。如果没有找到对应源 IP 地址的静态绑定表项；如果未匹配，则进行下一步处理。

命令：*display ip source binding*

例如：1.1.1.1 0002-0002-0002 的 ARP 报文会被丢弃，0011-1111-1111 1.1.1.1 报文符合静态绑定表项，会正常学到，其他 IP 地址非 1.1.1.1 的 ARP 正常学习。

```
<H3C>display ip source binding
Total entries found: 1
 MAC Address        IP Address                       VLAN   Interface    Type
 0011-1111-1111   1.1.1.1                            N/A    GE1/0/28    Static
```

（5）匹配 OUI-MAC、DOT1X、DHCP-SNOOPING

检查源 MAC 是否为 OUI-MAC，VOICE VLAN 是否使能；如果未匹配，则进行下一步处理。

命令：*display voice vlan oui*

display voice vlan state

例如：查看交换机上目前配置的 OUI-MAC 如下且端口 Ten-GigabitEthernet5/0/1 使能了 *voice vlan*。

```
[H3C]dis voice vlan oui
Oui Address        Mask            Description
0001-e300-0000   ffff-ff00-0000   Siemens phone
0003-6b00-0000   ffff-ff00-0000   Cisco phone
0004-0d00-0000   ffff-ff00-0000   Avaya phone
0060-b900-0000   ffff-ff00-0000   Philips/NEC phone
00d0-1e00-0000   ffff-ff00-0000   Pingtel phone
00e0-7500-0000   ffff-ff00-0000   Polycom phone
00e0-bb00-0000   ffff-ff00-0000   3com phone
[H3C]dis voice vlan state
 Maximum of Voice VLANs: 128
 Current Voice VLANs: 1
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                       VLAN          MODE          COS          DSCP
 -----------------------------------------------------------------------------
 Ten-GigabitEthernet5/0/1    2            AUTO          6            46
```

检查 IP、MAC 是否匹配 DHCP-SNOOPING 表项；如果未匹配，则进行下一步处理。

命令：*display dhcp-snooping*

例如：匹配 1.1.1.1 1111-1111-1111 的 ARP 正常学习，其符合 dhcp-snooping 表项。

```
[H3C]dis dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all ports.
 Type : D--Dynamic , S--Static , R--Recovering
```

```
Type IP Address        MAC Address      Lease VLAN SVLAN     Interface
 D     1.1.1.1     1111-1111-1111         286     1        2    GigabitEthernet1/0/1
------------------------------------------------------------------------------
---  --
```

检查源 MAC 是否为 dot1x 的 MAC。如果是,则正常学习;否则丢弃报文。

命令:*display connection access-type dot1x*

例如:源 MAC 2c59-e501-a055 是 dot1x 用户的 MAC。

```
[H3C]display connection access-type dot1x
Slot:   1
Index=23   , Username=dot1x@dot1x
 IP=N/A
 IPv6=N/A
 MAC=2c59-e501-a055

 Total 1 connection(s) matched on slot 1.
```

中低端设备CPU利用率高故障排查

孔天娇





1. 开始

本文档主要针对中低端 V5 平台产品，包括：Blade 5500、B6300、S3100V2、S3600V2、S3500-EA V2、S5120、S5500、CE3000、S5800、CE3000-EI、S5810、S5820X、S5830、S7500E、S7600、S7600-X V5、S10500 V5、部分 WX 系列产品、部分教育网 E 系列。

中低端产品出现 CPU 利用率高问题，首先应该查看导致 CPU 利用率异常高的 CPU 任务，如果是常见的导致 CPU 利用率高的 CPU 任务（排查步骤中有罗列），请按照本云图的指导，继续排查问题的具体原因；如果是非常见的 CPU 任务，请拨打 400-810-0504 寻求帮助。

对于 S7500、S7500E、S7600、S7600-X V5、S10500 V5 及 WX 系列产品这些框式设备，需要先判断是哪一类单板的 CPU 利用率异常高，如果是主控板和业务板，按照本云图继续排查；如果是 OAA 单板和功能单板（如 NAT 单板、NetStream 单板等），因为这些单板在正常情况下 CPU 利用率就偏高，所以不在本云图排查对象范围内，可以拨打 400-810-0504 寻求帮助。

2. 流程图相关操作说明

（1）判断设备或单板 CPU 利用率是否异常高

其中框式设备需要判断是主控板和业务板 CPU 利用率高，还是 OAA 单板和功能单板 CPU 利用率高。

命令：*display cpu*

① 正常情况下，盒式设备、框式设备业务板和主控板的 CPU 利用率一般都是在 60%以内的，应根据 CPU 5 分钟内的平均利用率来判断该设备或单板的 CPU 利用率是否异常。如果确认 CPU 利用率高，请按照后续步骤继续排查。

② 正常情况下，OAA 单板和功能单板（如 NAT 单板、NetStream 单板等）CPU 利用率偏高，不在本云图的排查对象范围内。

例如：通过命令可以判断出 3 号槽位的单板 CPU 利用率异常高。

```
<H3C>display cpu
Slot 0 CPU usage:
          11% in last 5 seconds
          13% in last 1 minute
          13% in last 5 minutes
Slot 3 CPU usage:
          85% in last 5 seconds
          79% in last 1 minute
          71% in last 5 minutes
```

（2）查看导致 CPU 利用率异常高的 CPU 任务

确认单板 CPU 利用率异常高后，需要查看导致单板 CPU 利用率异常高的 CPU 任务。

命令：*display cpu-usage 1 verbose（chassis　Chassis number）slot slot number*

从最新记录（倒数第一条记录）开始，显示 entry-number 条记录（下面的举例中是 5 条）。

例如：查询 slot 0 槽位单板的 5 条 CPU 利用率记录。

```
[H3C]display  cpu-usage 1 verbose chassis  1  slot  2
---------- CPU usage info (no:  0  idx: 16) ----------
CPU Usage Stat. Cycle : 60 (Second)
CPU Usage              :64%                              //CPU 使用率
CPU Usage Stat. Time : 2015-02-03  11:51:41              //查看时间
CPU Usage Stat. Tick  : 0xc39(CPU Tick High) 0x3872564(CPU Tick Low)
Actual Stat. Cycle     : 0x2(CPU Tick High) 0xcb458971(CPU Tick Low)

TaskName         CPU         Runtime(CPU Tick High/CPU Tick Low)
VIDL             36%              2/ 2a37179
TICK              0%              0/ 1309565
STMR              0%              0/  482b03
RECV              0%              0/  28210e
DSTK              0%              0/   182f4
SUBC              0%              0/    d85a
L2X0              2%              0/ 518ba64
bC.0              0%              0/ 1541da2
bLK0              0%              0/ 107b86b
DQFD              0%              0/  1c01e0
DQIT              0%              0/ 13b52b1
T_DM             40%             40/bcd37179
```

通过查询命令可以确认是 co0 任务引起 CPU 升高的(VIDL 是空闲任务),这时就要进一步排查 Console 用户进行了什么命令操作才导致的。

常见的导致 CPU 利用率异常高的 CPU 任务如表 5-14 所示。

表 5-14 导致 CPU 利用率高的任务

CPU 任务名	任 务 描 述
VIDL	空闲任务
T_DM	MAC 同步任务
L2X0/L2X1	地址同步任务
ROUT	路由管理任务
ARP	ARP 协议报文处理任务
co0	Console 口用户与设备之间的会话任务
vt0	Vty 用户与设备之间的会话任务

如果导致 CPU 利用率异常高的 CPU 任务在上述列表中,请按照后续步骤继续排查。

如果导致 CPU 利用率异常高的 CPU 任务不在上述列表中,说明该任务是非常见的导致 CPU 利用率异常高的 CPU 任务,请拨打 400-810-0504 寻求帮助。

(3) 判断导致 CPU 利用率异常高的原因,排除异常源

确认导致 CPU 利用率异常高的 CPU 任务后,就需要对常见的导致 CPU 利用率异常高的任务进行问题排查。

① L2X0/L2X1/ T_DM 任务,这些任务都和 MAC 地址学习相关,需要排查设备是否存在 MAC 地址漂移,或者设备收到大量 TC 报文,导致 MAC 地址频繁刷新。

对于 MAC 地址漂移问题,可以通过以下命令查看 MAC 地址迁移记录。

命令: *debugl2 slot_id chip mac/move_rec/show*(诊断视图)

例如: 查看 S75E slot 5 MAC 地址迁移记录。

```
[H3C-diagnose]debug l2 5 0 mac/move_rec/show
------------------------------- L2MACMOVEMODULE  INFO ----------------------
L2MacMoveModule Enabled
L2MacMoveDebug Switch Off
------------------------------- L2MACMOVE Record  INFO ----------------------
MacAddress         Vlan Agg Mod Port ->Agg Mod Port Cnt LatestTime       Del
0 :e0:4c:17:f4:9e 20    0   14   3    ->0   14   9    4   2015/1 /9  10:24:22 1
0 :e0:4c:17:f4:58 30    0   10   11   ->0   15   4    6   2015/1 /9  10:24:24 1
0 :e0:4c:17:f4:5c 20    0   10   3    ->0   14   20   6   2015/1 /9  10:24:50 1
0 :e0:4c:17:f5:66 10    0   10   0    ->0   14   2    2   2015/1 /9  10:24:50 1
0 :e0:4c:17:f5:24 30    0   10   11   ->0   15   7    7   2015/1 /9  10:24:59 1
0 :e0:4c:17:f5:2c 30    0   10   9    ->0   15   10   6   2015/1 /9  10:25:22 1
```

从以上标红的信息中可以看到 0 :e0:4c:17:f4:9e（补全为 00e0-4c17-f49e)这个 MAC 地址在 vlan 20 内、聚合组 0(实际为非聚合组成员端口)，从 MOD 14 的 PORT 3 漂移至 MOD 14 的 PORT 9，漂移次数为 4 次，最后一次漂移时间为 2015/1/9 10:24:22。

查看漂移的实际物理端口还需要结合[h3c-diagnose]debug port mapping slot_id 命令。

```
[H3C-diagnose] debug port mapping 5
 [Interface]    [Unit] [Port] [Name] [Combo?] [Active?] [IfIndex] [MID] [Link] [Attr]
--------------------------------------------------------------------------------------
 GE5/0/1          0      1     ge1    no        no     0x2900000  14    up    Bridge
 GE5/0/2          0      0     ge0    no        no     0x2900001  14    up    Bridge
 GE5/0/3          0      3     ge3    no        no     0x2900002  14    up    Bridge
 GE5/0/4          0      2     ge2    no        no     0x2900003  14    up    Bridge
 GE5/0/5          0      5     ge5    no        no     0x2900004  14    up    Bridge
 GE5/0/6          0      4     ge4    no        no     0x2900005  14    up    Bridge
 GE5/0/7          0      7     ge7    no        no     0x2900006  14    up    Bridge
 GE5/0/8          0      6     ge6    no        no     0x2900007  14    up    Bridge
 GE5/0/9          0      9     ge9    no        no     0x2900008  14    up    Bridge
 GE5/0/10         0      8     ge8    no        no     0x2900009  14    up    Bridge
 GE5/0/11         0      11    ge11   no        no     0x290000a  14    up    Bridge
 GE5/0/12         0      10    ge10   no        no     0x290000b  14    up    Bridge
 GE5/0/13         0      13    ge13   no        no     0x290000c  14    up    Bridge
 GE5/0/14         0      12    ge12   no        no     0x290000d  14    up    Bridge
 GE5/0/15         0      15    ge15   no        no     0x290000e  14    up    Bridge
 GE5/0/16         0      14    ge14   no        no     0x290000f  14    up    Bridge
 GE5/0/17         0      17    ge17   no        no     0x2900010  14    up    Bridge
 GE5/0/18         0      16    ge16   no        no     0x2900011  14    up    Bridge
 GE5/0/19         0      19    ge19   no        no     0x2900012  14    up    Bridge
 GE5/0/20         0      18    ge18   no        no     0x2900013  14    up    Bridge
 GE5/0/21         0      21    ge21   no        no     0x2900014  14    up    Bridge
 GE5/0/22         0      20    ge20   no        no     0x2900015  14    up    Bridge
```

从以上映射关系可以看到，之前的从 MOD 14 的 PORT 3 漂移至 MOD 14 的 PORT 9，实际的物理漂移为从 GE5/0/3 漂移至 GE5/0/9。存在 MAC 漂移，一般为存在环路导致，因此需要在这几个端口之间排查底下的设备是否存在环路。

涉及聚合口的漂移的查看稍微有些区别，这里不详细介绍。可参看中低端常见故障处理胶片。

对于设备收到大量 TC 报文问题，可通过以下命令多次查看使能 STP 的端口 TC 报文的收发情况。

命令：<*H3C*>*dis stp tc slot slot_id*

例如：查看 slot 3 的 TC 告警信息。

```
<H3C>display stp  tc  slot  3
-------------- STP slot 3 TC or TCN count -------------
MSTID    Port                       Receive     Send
  0      GigabitEthernet3/0/1         0          39
  0      GigabitEthernet3/0/2        24          45
  0      GigabitEthernet3/0/3         0          41
```

② ROUT 任务，路由管理任务，需要排查设备是否存在路由振荡问题。通过以下命令可以查询路由表统计信息，如果路由增删计数变化明显，请排查相关路由协议振荡源。

命令：*display ip routing-table statistics*

例如：查看设备的路由表统计信息。

```
<H3C>display ip routing-table statistics
Protocol   route    active    added    deleted    freed
DIRECT      24        4        25        1          0
STATIC      3         0         3        0          0
RIP         0         0         0        0          0
OSPF        12        6         0        0          0
IS-IS       0         0         0        0          0
BGP         0         0         0        0          0
Total       39       10        28        1          0
```

③ ARP 任务，处理 ARP 协议报文的任务，需要排查是否存在 ARP 攻击问题。通过以下命令可以查询上送 CPU 的 ARP 报文的情况，包括 ARP 收包速率、被丢弃报文个数，需要多次查看，观察增长情况。

命令：*debug rxtx softcar showshot_id*（诊断视图）

例如：查看设备 slot 5 上送 CPU 报文统计，重点关注 ARP 报文

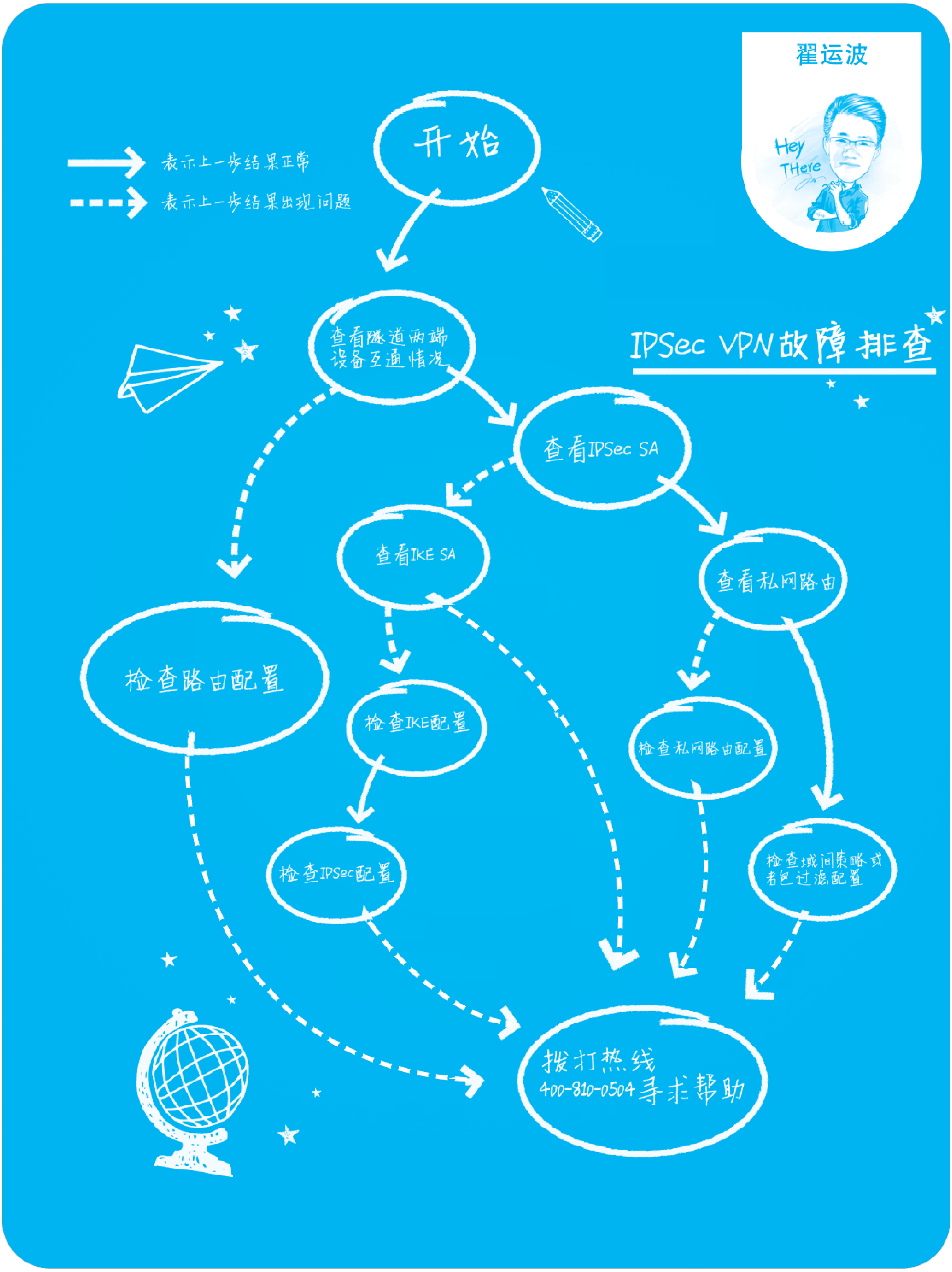
```
[H3C-diagnose] debug rxtx softcar show 5
----------------------------------------------------------------------------------
 The softcar pps auto-adjust switch: On
 ID   Type         Pkt_PSec DisPkt_All Pps   Dynamic Switch Hash   ACLmax
 0    ROOT         0        0          200   S       On     SMAC 0
 1    ISIS         0        0          200   D       On     SMAC 8
 …
 29   ARP          35       25670      100   S       On     SMAC 8
 30   ARP_REPLY    0        0          100   S       On     SMAC 8
```

④ co0/vt0 任务，Console 口用户或者 vty 接口用户（比如 Telnet 用户）与设备之间的会话任务，需要确认 Console 口用户或者 vty 接口用户（比如 Telnet 用户）是否正在收集诊断信息、用复制粘贴方式下发大量配置等操作。如果有相关操作，请停止相关操作后再观察单板的 CPU 利用率是否恢复正常。

如果排除以上问题后，单板 CPU 利用率还存在异常高的问题，请拨打 400-810-0504 寻求帮助。

06

安全产品



翟运波
Hey THere
IPSec VPN故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看隧道两端设备互通情况
查看IPSec SA
查看IKE SA
查看私网路由
检查路由配置
检查IKE配置
检查私网路由配置
检查IPSec配置
检查域间策略或者包过滤配置
拨打热线 400-810-0504寻求帮助

06 安全产品 > 6.1 安全协议 > 6.1.1 IPSec VPN 故障排查 > 步骤详解

1. 开始

IPSec VPN 是一种很常用的三层 VPN 技术，它可以保证数据通信的机密性、完整性，还可以实现数据源验证、防重放报文等安全功能。IPSec VPN 的相关问题需要综合考虑路由、IKE、IPSec 和访问控制等模块，定位故障的思路是：先查路由，再查 IKE 和 IPSec 模块，最后查看安全策略。

2. 流程图相关操作说明

(1) 查看隧道两端设备互通情况

要想保证 IPSec VPN 隧道建立成功，首先需要保证隧道两端设备通信正常，IKE 协议报文(UDP 端口 500 或者 4500)能够正常交互。先查看两端 VPN 设备的路由或者通过 ping 等手段测试网络互通情况，然后检查对端设备及中间防火墙的配置确保 UDP 500 或者 4500 端口开放。在本地可以通过抓包或者 debug IKE 的方法确认是否收到对端设备发送的 IKE 报文，但是如果设备配置多个 IKE Peer 时，不建议采用 debug IKE 的方法。

命令：*ping x.x.x.x*

```
<H3C>ping60.191.99.142
  PING60.191.99.142: 56   data bytes, press CTRL_C to break
    Reply from60.191.99.142: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from60.191.99.142: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from60.191.99.142: bytes=56 Sequence=2 ttl=255 time=1 ms
```

(2) 检查公网路由

如果不能 ping 通隧道对端地址，或者无法收到对端发送的 IKE 报文，需要检查两端设备之间的路由和安全策略配置。不同设备的安全策略配置不同，具体参考对应设备的配置手册。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看本地设备到达隧道对端地址 60.191.99.142 的路由是否正常。

```
<H3C>display ip routing-table 60.191.99.142
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto  Pre  Cost        NextHop         Interface
60.191.99.0/24      Direct  0    0          60.191.99.141   GE0/1
```

(3) 查看 IPSec SA

如果 IPSec SA 是通过手工建立的，需要仔细查看两端设备 SA 的相关参数配置是否正确，如果 IPSec SA 是通过 IKE 协议动态协商的，那么需要查看两端 IPSec SA 是否已经建立，并检查两端 SA 的 SPI、保护的数据流等信息是否匹配。正常情况下两端设备的 Inbound 和 Outbound SA 是相互对应的，保护数据流(flow)的源目的地址也是相反的。

命令：*display ipsec sa* {*brief*|*remote*}

例如：通过命令查看，可以确认 IPSec VPN 的 SA 已经正常建立，SPI 和保护的数据流(FLOW)都是正确的。

```
[H3C]display ipsec sa
-------------------------------
  Interface: GigabitEthernet0/1
    path MTU: 1500
-------------------------------


  -----------------------------
  IPsec policy name: "ipsecvpn"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  -----------------------------
    connection id: 8
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 60.191.99.141
        remote address: 60.191.99.142
    flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 192.168.2.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 1893507505 (0x70dca1b1)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843159/2953
      max sequence number received: 641
      anti-replay check enable: Y
      anti-replay window size: 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 438707633 (0x1a2625b1)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843159/2953
      max sequence number sent: 642
      udp encapsulation used for nat traversal: N
```

（4）查看 IKE SA

查看 VPN 设备上 IKE 第一阶段和第二阶段 SA 是否建立正常。

命令：*display ike sa* {*verbose*}

例如：通过命令查看，可以确认 IKE 第一阶段和第二阶段的 SA 已经正常建立。

```
[H3C]display ike sa
    total phase-1 SAs:   1
    connection-id  peer                    flag          phase     doi
  --------------------------------------------------------------------------
     58            60.191.99.142           RD            1         IPSEC
     59            60.191.99.142           RD            2         IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

（5）检查 IKE 配置

检查 VPN 隧道两端设备 IKE 相关配置是否正确，包括 ike local-name、ike proposal 以及 ike peer 等配置。

命令：*display current-configuration/include ike*

display ike proposal

diplay ike peer

例如：通过命令查看 ike local-name、ike proposal、ike peer 等相关配置是否正确。

```
[H3C] display current-configuration| include ike
#
 ike local-name beijing
#
[H3C]display ike proposal
 priority  authentication  authentication  encryption  Diffie-Hellman  duration
               method          algorithm       algorithm       group          (seconds)
---------------------------------------------------------------------------------------
   1        PRE_SHARED        MD5            3DES_CBC        MODP_768      86400
  default   PRE_SHARED        SHA            DES_CBC         MODP_768      86400
[H3C]display ike peer
---------------------------
IKE Peer: hangzhou
   exchange mode: aggressive on phase 1
   proposal: 1
   pre-shared-key ******
   peer id type: name
   peer ip address: 60.191.99.142
   local ip address:
   peer name: hangzhou
   nat traversal: enable
   dpd:
---------------------------
```

（6）检查 IPSec 配置

查看隧道两端设备 IPSec 策略的封装模式、加密及认证方式是否一致，保护的数据流是否对应，以及 IPSec 策略是否正确下发等内容。

命令：*display acl number*

display ipsec transform-set

display ipsec policy

display current-configuration interface interface-type interface-number

例如：通过命令查看 IPSec 的 ACL、安全协议、加密认证算法等相关配置。

```
[H3C]display acl 3000
Advanced ACL  3000, named -none-, 1 rule,
ACL's step is 5
rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255(10 times matched)
[H3C]display ipsec transform-set

IPsec transform-set name: bjhz
    encapsulation mode: tunnel
    ESN : disable
```

```
        ESN scheme: NO
        transform: esp-new
        ESP protocol:
          Integrity: sha1-hmac-96
          Encryption: 3des
[H3C]display ipsec policy
-------------------------------
  IPsec Policy Group: "ipsecvpn"
  Interface: GigabitEthernet0/1
-------------------------------
  -----------------------------
  IPsec policy name: "ipsecvpn"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  -----------------------------
    security data flow : 3000
    selector mode: standard
    ike-peer name:   hangzhou
    perfect forward secrecy:
    transform-set name:   bjhz
    synchronization inbound anti-replay-interval: 1000 packets
    synchronization outbound anti-replay-interval: 100000 packets
    IPsec sa local duration(time based): 3600 seconds
    IPsec sa local duration(traffic based): 1843200 kilobytes
    policy enable: True
    tfc enable: False
[H3C]display current-configuration interface GigabitEthernet 0/1
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 60.191.99.141 255.255.255.0
 ipsec policy ipsecvpn
#
```

（7）检查私网路由

私网路由就是指被 IPSec VPN 保护的数据流的路由，主要是查看两端 VPN 设备到站点之间的路由是否正常，VPN 设备上到对端私网的路由是否从配置 IPSec 策略的接口出去等信息。

命令：*display ip routing-table*

例如：通过命令查看，可以确认 VPN 设备到达本端私网网段 192.168.1.0/24 的路由正常，到达对端私网网段 192.168.2.0/24 的路由也已经存在，而且出接口就是下发 IPSec VPN 策略的接口。

```
[H3C]display ip routing-table
Routing Tables: Public
        Destinations : 7          Routes : 7

Destination/Mask     Proto  Pre  Cost      NextHop         Interface

60.191.99.0/24       Direct 0    0         60.191.99.141   GE0/1
60.191.99.141/32     Direct 0    0         127.0.0.1       InLoop0
192.168.1.0/24       Direct 0    0         192.168.1.1     GE0/2
192.168.1.1/32       Direct 0    0         127.0.0.1       InLoop0
192.168.2.0/24       Static 60   0         60.191.99.142   GE0/1
```

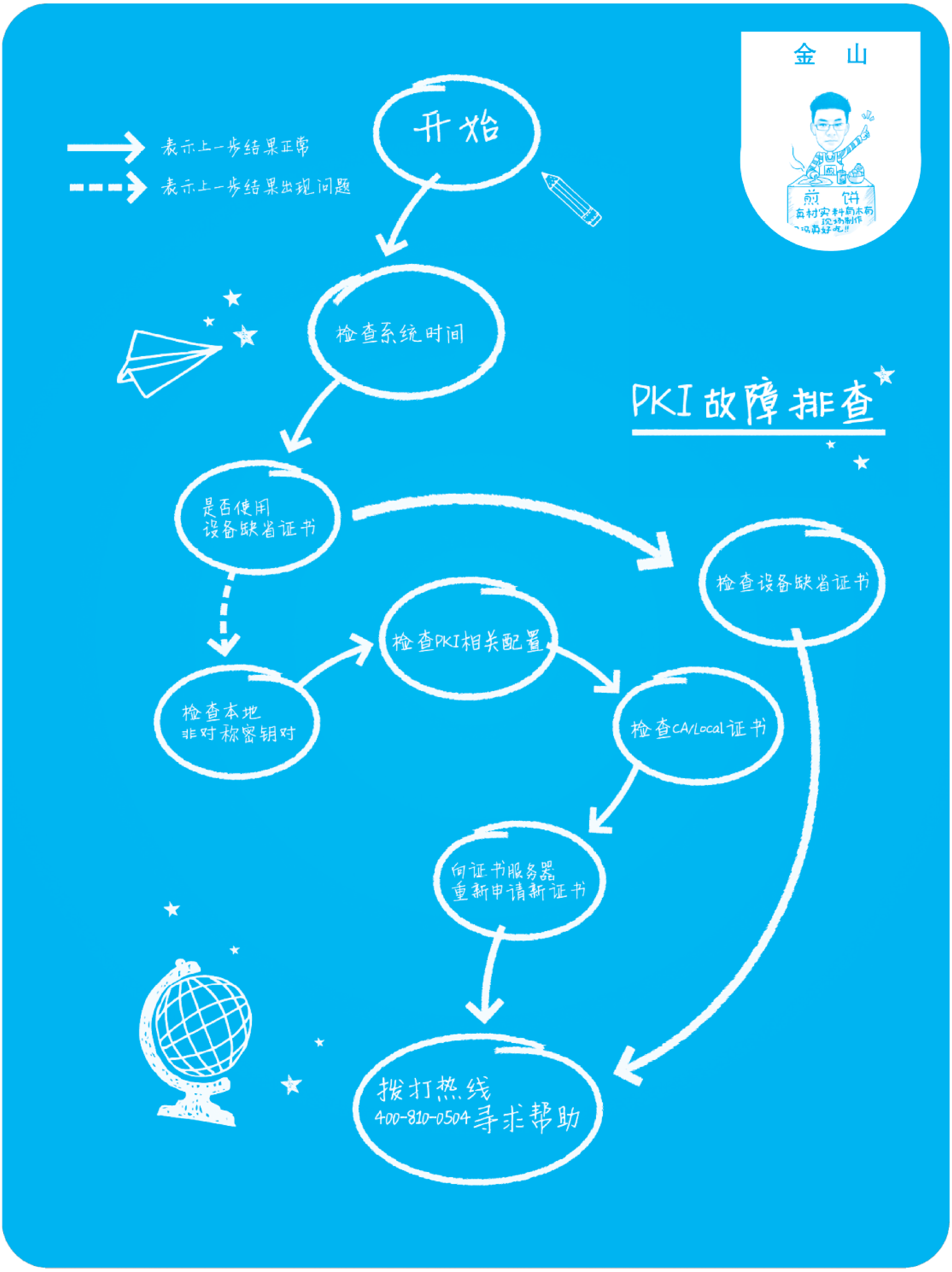
（8）检查域间策略或者包过滤配置

在某些情况下有可能会在设备上配置 IPSec VPN 的同时也配置了相关包过滤或者域间策略等功能，为了保证 IPSec VPN 隧道能够正常建立和通信，需要在配置包过滤策略时允许 IPSec VPN 的协议报文以及加解密后的数据报文通过。

命令：*display current-configuration*

例如：以防火墙为例，设备配置了 Untrust 到 Trust 的域间策略并允许所有报文通过，所以不会阻断 IPSec VPN 的协议报文及加密后的数据报文。

```
[H3C]display current-configuration
#
vd Root id 1
#
zone name Trust id 2
 priority 85
 import interface GigabitEthernet0/2
zone name DMZ id 3
 priority 50
zone name Untrust id 4
 priority 5
 import interface GigabitEthernet0/1
switchto vd Root
interzone source Untrust destination Trust
rule 0 permit
source-ip any_address
destination-ip any_address
service any_service
rule enable
#
```


金 山
表示上一步结果正常
表示上一步结果出现问题
开始
检查系统时间
PKI故障排查
是否使用
设备缺省证书
检查设备缺省证书
检查PKI相关配置
检查本地
非对称密钥对
检查CA/Local证书
向证书服务器
重新申请新证书
拨打热线
400-810-0504寻求帮助

1. 开始

PKI 问题定位故障的思路是：依次检查系统时间、本地公私钥对、PKI 相关配置是否正确，然后检查系统是否获得了正确的 CA/Local 证书，若没有获得证书则应重新向 CA/RA 服务器进行申请。若客户没有 CA/RA 服务器，希望直接使用设备默认的数字证书，则可以检查设备系统默认证书是否已经生成且有效。

2. 流程图相关操作说明

(1) 检查系统时间

查看设备的当前系统时间、时区等设备是否正确。

命令：*display clock*

例如：通过命令查看当前设备的系统时间是否正确。

```
<H3C> display clock
09:34:11Beijing Fri 05/03/2013
Time Zone :Beijing add 08:00:00
```

若系统时间不正确应该立即调整，建议启用 NTP 服务为设备实时同步时钟。

命令：*clock datetime xx:xx xxxx/xx/xx*

例如：通过命令设置系统时间。

```
<H3C> clock datetime 10:12 2013/05/03
```

(2) 检查本地非对称密钥对

查看本端设备当前是否存在本地 RSA/DSA 非对称密钥对。

命令：*display public-key local rsa public*

若执行命令后，命令行界面上无任何对应输出，则说明系统当前没有生成相应的非对称密钥对。应当手工操作重新生成或通过导入携带私钥的证书获取。

例如：通过命令查看当前设备的 RSA 密钥对。

```
<H3C>display public-key local rsa public
--------------------------------------------------------------------------------
Time of Key pair created: 03:11:19   2013/05/02
Key name: HOST_KEY
Key type: RSA Encryption Key
--------------------------------------------------------------------------------
Key code:
...
--------------------------------------------------------------------------------
Time of Key pair created: 03:11:21   2013/05/02
Key name: SERVER_KEY
Key type: RSA Encryption Key
--------------------------------------------------------------------------------
```

```
Key code:
…
```

(3) 检查 PKI 相关配置

系统中的 PKI 相关配置主要分为两大部分：PKI 实体配置、PKI 域配置。排错过程中，可依据配置需求，对照用户手册检查各项配置是否完整。

① PKI 实体主要配置项为通用名、FQDN、email address 等，建议根据实际情况完整配置各属性值。

命令：*display current-configuration configuration pki-entity*

例如：通过命令查看 PKI 实体“aaa”的配置是否正确。

```
<H3C> dis current-configuration configuration pki-entity
#
pki entity aaa
  common-name firewall
#
```

② PKI 域主要配置项为信任的 CA 名、指定 PKI 实体名、证书申请的注册受理机构、注册服务器 URL 等，若组网环境中无 CRL 验证条件，需在 PKI 域中配置禁用 CRL 验证。

命令：*display current-configuration configuration pki-domain*

例如：通过命令查看 PKI 域“torsa”的配置是否正确。

```
<H3C> display current-configuration configuration pki-domain
#
pki domain torsa
  ca identifier myca
  certificate request url http://1.1.1.1:8080/certsrv/mscep/mscep.dll
  certificate request from ra
  certificate request entity aaa
#
```

说明：当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件，配置 PKI domain 时需要使用 certificate request from ra 命令指定实体从 RA 注册申请证书；当采用 RSA Keon 软件时，不需要安装 SCEP 插件，配置 PKI domain 时需要使用 certificate request from ca 命令指定实体从 CA 注册申请证书。

(4) 检查 CA/Local 证书

① 在确认配置无误的前提下，可通过 display 命令查看相应 PKI 域当前是否有 CA/Local 证书。

命令：*display pki certificate ca domain torsa*

例如：通过命令检查 PKI 域“torsa”所对应的 CA 证书是否存在。

```
[H3C] display pki certificate ca domain torsa
Certificate:
    Data:
        …
        Issuer:
            CN=myca
```

```
        Validity
            Not Before: Nov  9 01:48:34 2007 GMT
            Not After : Nov  9 01:48:34 2017 GMT
        Subject:
            CN=myca
        …
```

② 系统支持通过命令在本地对证书进行即时验证，以帮助网络管理员判断数字证书是否合法有效。如果 CA/Local 证书不能通过系统验证，则必须重新申请有效证书。

命令：*pki validate-certificate ca domain torsa*

例如：通过验证命令检查 PKI 域"default"所对应的 CA 证书是否有效。

```
[H3C] pki validate-certificate ca domain torsa
Verifying certificate...
        Serial Number:
            4D6D8894 4303D582 4385962F A336BE22
        Issuer:
            CN=myca
        Subject:
            CN=myca

Verify result: ok
```

（5）向证书服务器重新申请新证书

若系统当前 PKI 域所使用的 CA/Local 证书因超期、私钥泄露等原因无效，则应重新向证书服务器申请新证书。建议在重新申请证书前，先为设备重新生成新的本地非对称密钥对。

① 若 CA 服务器与设备 IP 可达，可以直接在线申请并获取证书。申请成功后将 CA/Local 证书通过 IP 网络直接下载至本地 PKI 域。若服务器没有部署自动颁发证书机制，则在线申请证书后还需服务器侧操作为该次申请颁发证书（具体操作方式需查看服务器相关说明）。索取证书时要注意顺序，先下载 CA 证书，然后再下载 Local 证书。

命令：*pki retrieval-certificate* { *ca* | *local* } *domain XXX*

pki request-certificate domain torsa challenge-word

例如：设备通过在线方式直接向 CA 服务器发起证书申请，服务器颁发证书后下载至本地 PKI 域"torsa"。

```
[H3C] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while...
The trusted CA's finger print is:
MD5 fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4
Is the finger print correct?(Y/N): y
Saving CA/RA certificates chain, please wait a moment...
CA certificates retrieval success.

[H3C] pki request-certificate domain torsa challenge_word
Certificate is being requested, please wait...

Enrolling the local certificate,please wait a while...
```

```
Certificate request successfully!
Saving the local certificate to device...
Done!
```

② 若 CA 服务器与设备间无法通过 IP 网络互通，则可以通过离线申请方式，将设备上生成的 pkcs10 格式的证书申请带外传递到服务器上；待 CA 服务器成功颁发证书后，再通过带外方式将证书上传回设备存储介质，然后再通过命令导入 PKI 域，在导入时要注意选择正确的证书文件格式。

命令：*pki import-certificate* { *ca* | *local* } *domain torsa der filename myca.cer*

例如：通过命令将以带外方式上传至设备存储介质的数字证书导入 PKI 域“torsa”。

```
[H3C] pki import-certificate ca domain torsa der filename myca.cer
Importing certificates. Please wait a while...

The trusted CA's finger print is:
    MD5  fingerprint:9B23 87B8 96FF BEC5 EE9D 03D0 6586 A8F1
    SHA1 fingerprint:15D0 859F A5D6 9F20 7913 09BB E002 3215 B7AA DD60

Is the finger print correct?(Y/N): y
.
%Nov 12 16:53:47:889 2007 H3C PKI/4/Verify_CA_Root_Cert: CA root certificate of the domaintorsa is trusted...
Import CA certificate successfully.
```

(6) 检查设备默认证书

设备以默认的空配置首次启动时会自动创建本地非对称密钥对，并生成与默认的 PKI 域“default”相对应的 CA、Local 证书。可通过命令检查默认证书是否已经创建。

命令：*display pki certificate ca domain default*

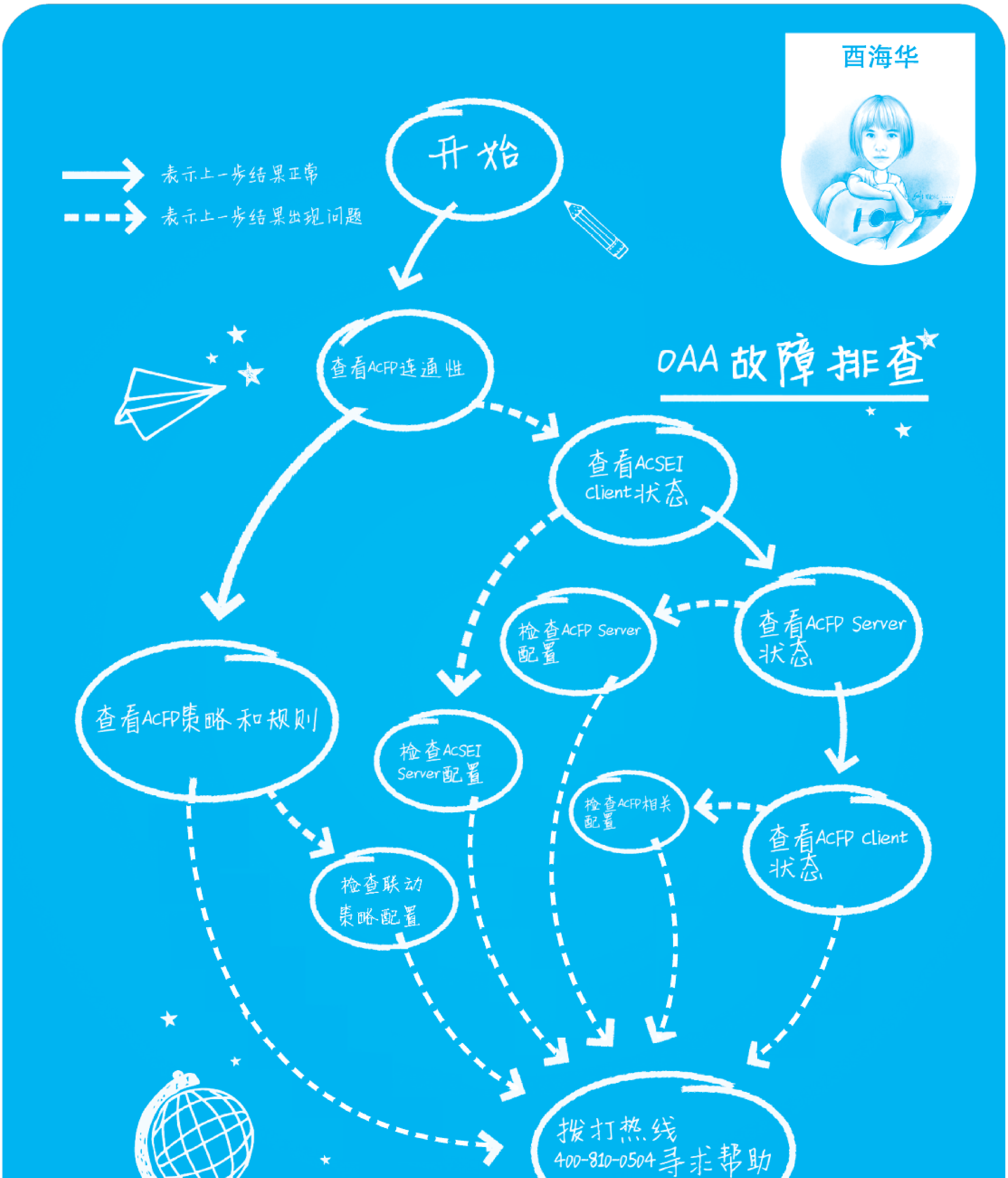
例如：通过命令查看默认 CA 证书，其 CN 名通常为“cademo”，有效期一般为 10 年。

```
<H3C>display pki certificate ca domain default
Certificate:
    Data:
        ...
        Issuer:
            CN=cademo
        Validity
            Not Before: Nov  9 01:48:34 2007 GMT
            Not After : Nov  9 01:48:34 2017 GMT
        Subject:
            CN=cademo
        ...
```

例如：通过命令查看默认 Local 证书，其 CN 名通常为“cademo”，有效期一般为 10 年。

```
<H3C>display pki certificate local domain default
Certificate:
    Data:
        ...
        Issuer:
```

```
        CN=cademo
    Validity
        Not Before: Nov 12 07:34:55 2007 GMT
        Not After : Nov  9 01:48:34 2017 GMT
    Subject:
        C=CN
        ST=localdemo
        L=localdemo
        O=localdemo
        OU=localdemo
        CN=localdemo
    …
```


西海华
OAA 故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看ACFP连通性
查看ACSEI client状态
查看ACFP Server状态
检查ACFP Server配置
查看ACFP策略和规则
检查ACSEI Server配置
检查ACFP相关配置
查看ACFP Client状态
检查联动策略配置
拨打热线 400-810-0504寻求帮助

1. 开始

OAA 架构通过 ACFP 联动实现，ACFP 联动提供了一套机制，使得 Secblade IPS/ACG 通过向交换机下发联动策略规则，将交换机的流量重定向或镜像到 SecBlade IPS/ACG，完成处理后再返回给交换机或丢弃。OAA 问题定位故障的思路是：首先是保证 ACFP 联动成功，其次是保证联动策略和联动规则的正确下发。

2. 流程图相关操作说明

(1) 查看 ACFP 连通性

登录 ACFP Client 设备 Web 页面，进入菜单，单击“系统管理”→“网络管理”→“ACFP Client 配置”命令，单击“连通性测试”按钮，如图 6-1 所示。

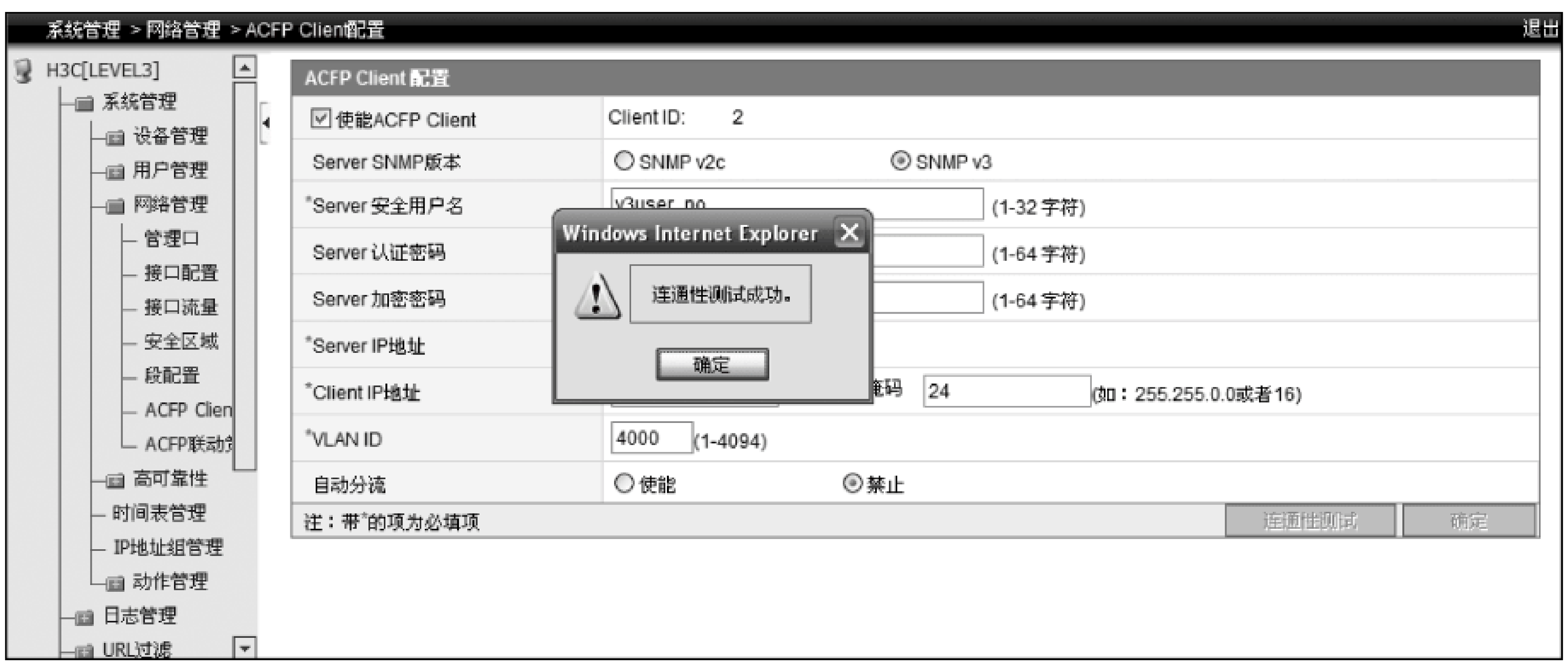


图 6-1 ACFP Client 配置

(2) 检查 ACSEI Client 状态

查看 acsei client 是否正确注册。

命令：*display acsei client info*

例如：通过命令查看，可以确认 acsei client 已正确注册。

```
<H3C>display acsei client info
 Total Client Number:1
 Client ID:2
 Client Description: Intrusion Prevention System
 Hardware: 2.0
 System Software: i-Ware software, Version 1.10
 Application Software: Ess 2113P03
 CPU: RMI XLR732
 PCB Version: Ver. A
 CPLD Version: 2.0
 Bootrom Version: 1.19
 Storage Card: 999MB
 Memory: 2002MB
 Harddisk: 0MB
```

（3）检查 ACSEI Server 相关配置

① 检查交换机上是否配置了命令 acsei server enable。

```
[H3C]display current-configuration | include acsei
acsei server enable
```

② 检查内联口是否配置扩展模式，以 S7500E 为例(其他交换机配置请参照相关文档)。

```
[H3C]display current-configuration interface Ten-GigabitEthernet 3/0/1
#
interface Ten-GigabitEthernet3/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4000
 port connection-mode extend
 stp disable
 mac-address mac-learning disable
#
```

（4）查看 ACFP Server 状态

查看 ACFP Server 状态。

命令：*display acfp server-info*

例如：通过命令查看，可以确认 ACFP Server 状态是否正常。

```
<H3C>display acfp server-info
Server-Info:        ipserver   redirect   mirror
Max Life-Time:      2147483647(s)
PersistentRules:    false
ContextType:        HGPlus-context
```

（5）检查 ACFP Server 配置

检查交换机上是否配置命令：acfp server enable。

```
<H3C>display current-configuration | include acfp
acfp server enable
```

（6）查看 ACFP Client 状态

查看 ACFP Client 状态。

命令：*display acfp client-info*

例如：通过命令查看，可以确认 ACFP Client 状态是否正常。

```
<H3C>display acfp client-info
ACFP client total number: 1
ClientID:      2
Description:  Application Control Gateway
Hw-Info:       2.0
OS-Info:       i-Ware software, Version 1.10
App-Info:      Ess 2113P03
Client IP:     172.31.255.11
Client Mode: redirect   mirror
```

(7) 检查 ACFP 相关配置

确认 ACFP Server 与 ACFP Client 通信 VLAN 地址是否能 ping 通，并查看相关配置是否都配置正确。

例如：通过命令 ping 查看通信 VLAN 连通性。

```
<H3C>ping 172.31.255.11
  PING 172.31.255.11: 56   data bytes, press CTRL_C to break
    Reply from 172.31.255.11: bytes=56 Sequence=0 ttl=64 time=2 ms
    Reply from 172.31.255.11: bytes=56 Sequence=1 ttl=64 time=1 ms
```

① 检查交换机配置，包括 SNMP 配置、内连口配置、mib-style 等，以 S7500E 为例(其他交换机配置略有差别，请参照相关文档)。

```
<H3C>display current-configuration | include snmp
 snmp-agent
 snmp-agent local-engineid 800063A2033CE5A682C521
 snmp-agent sys-info version v3
 snmp-agent group v3 v3group_no read-view iso write-view iso notify-view iso
 snmp-agent mib-view included iso iso
 snmp-agent usm-user v3 v3user_no v3group_no

<H3C>display current-configuration interface Ten-GigabitEthernet 4/0/1
#
interface Ten-GigabitEthernet4/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 4000
 port connection-mode extend
 stp disable
 mac-address mac-learning disable
#
<H3C>display mib-style
Current MIB style: new
Next reboot MIB style: new          //该配置配置完成后需要重启设备生效

<H3C>display current-configuration | include switch-mode
switch-mode l2-enhanced             //该配置配置完成后需要重启设备生效
```

② 检查 ACFP Client 配置，如图 6-2 所示。

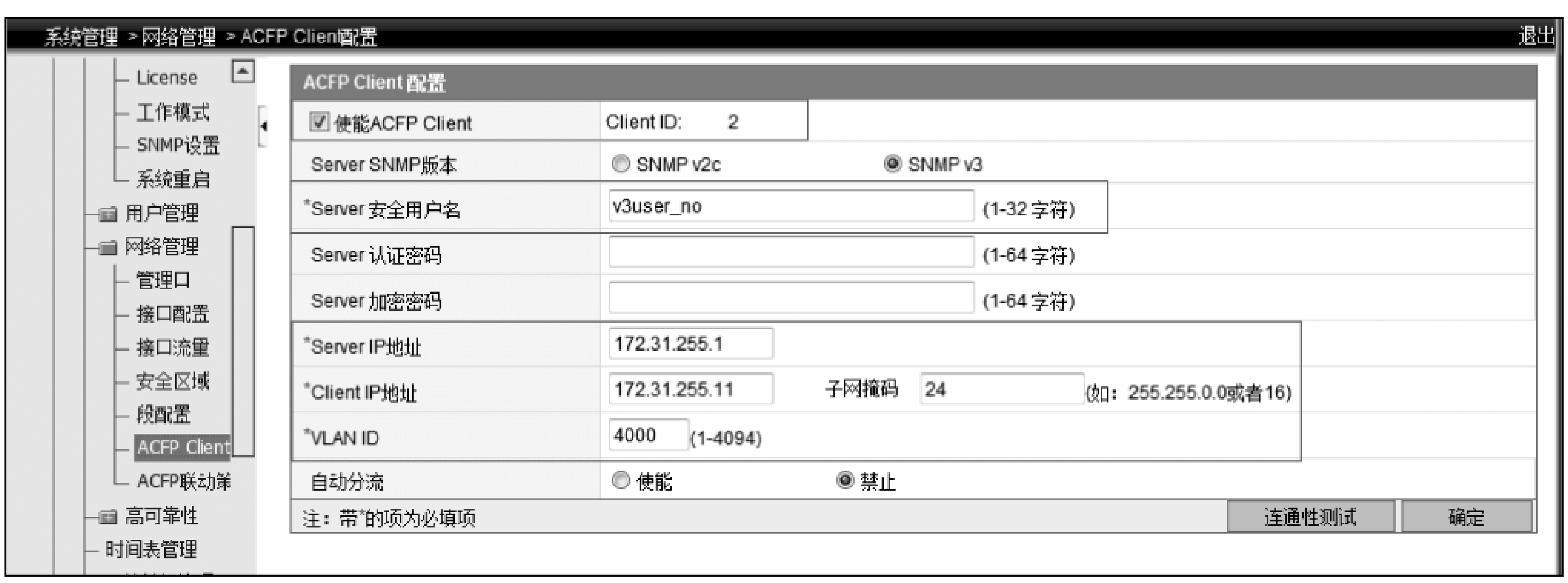


图 6-2 ACFP Client 配置

Server 安全用户名与交换机上 SNMP 配置保持一致。

```
snmp-agent usm-user v3 v3user_no v3group_no
```

Server IP 地址和 vlan 与交换机上通信 vlan 配置保持一致。

```
interface Vlan-interface 4000
ip address 172.31.255.1 255.255.255.0
```

Client IP 地址与 Server IP 地址配置在同一网段。

(8) 查看 ACFP 策略下发和规则下发状态

查看 ACFP 策略下发和规则下发状态。

命令：*display acfp policy-info*

display acfp rule-info interface interface-type interface-number

例如：通过命令查看，可以确认 ACFP 策略和规则已经正确下发。

```
[S7500E]display acfp policy-info
ACFP policy total number: 1
ClientID:          2                    Policy-Index:   1
Rule-Num:          1                    ContextID:      2050
Exist-Time:        17320(s)             Life-Time:      2147483647(s)
Start-Time:        00:00:00             End-Time:       24:00:00
Admin-Status:      enable               Effect-Status:  active
DstIfFailAction:   delete               Priority:       4
In-Interface:      GigabitEthernet2/0/1
Out-Interface:
Dest-Interface:    Ten-GigabitEthernet3/0/1

[S7500E]display    acfp rule-info interface GigabitEthernet 2/0/1
In-Interface:      GigabitEthernet2/0/1
ACFP rule total number:   1

ClientID:2                 Policy-Index:1           Rule-Index:1
StartVLAN: 1001            EndVLAN: 1001
TypeOrLen:2048
Action:redirect            Status:active            OperationStatus:succeeded
```

(9) 检查联动策略和规则

① 检查联动策略是否正确配置，内外部域接口分别配置对应策略，如图 6-3 所示。

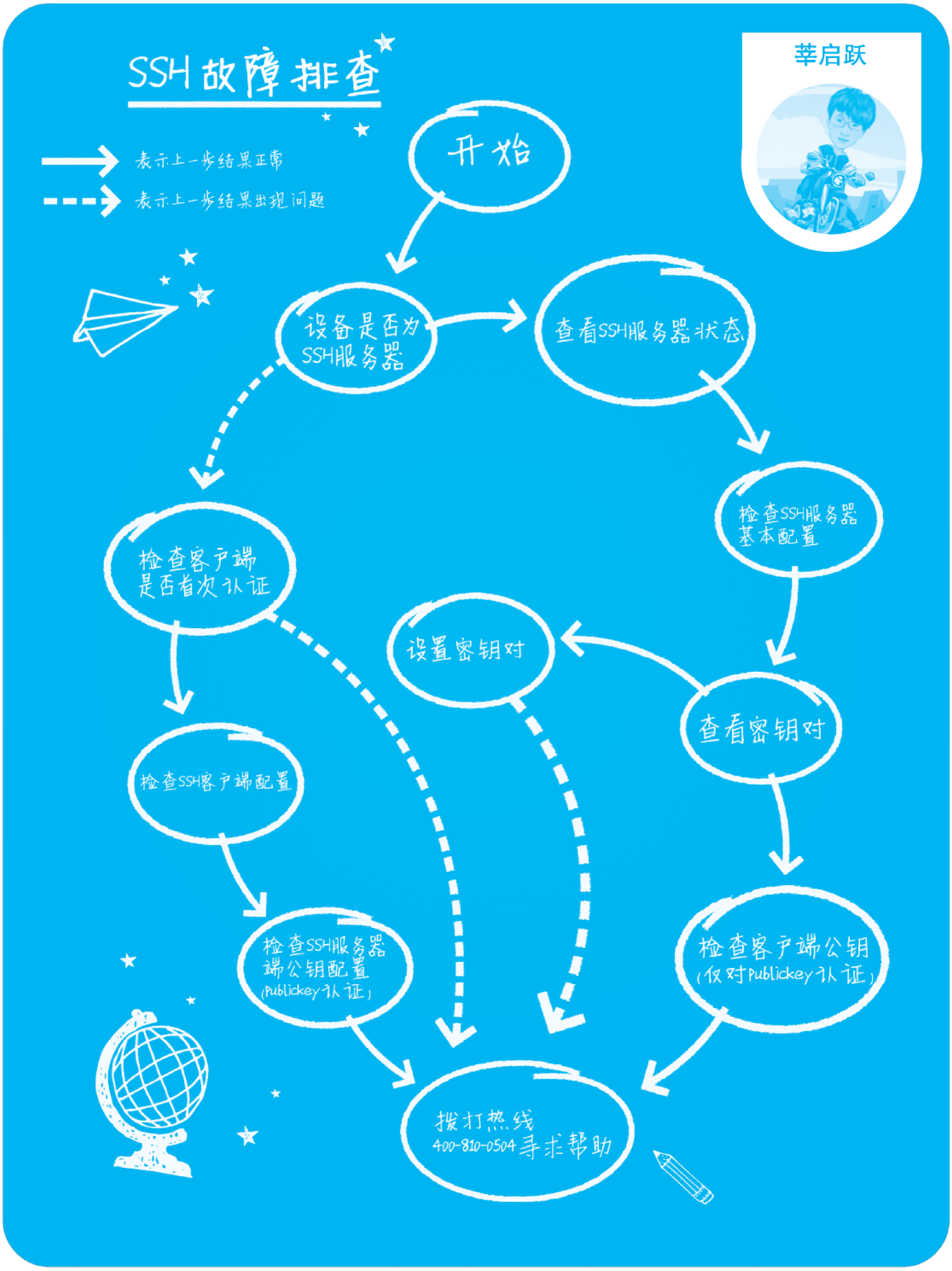


图 6-3　ACFP 联动策略(1)

② 检查联动规则是否正确配置，每个联动策略必须配置联动规则引流才能生效，如图 6-4 所示。



图 6-4　ACFP 联动策略(2)


SSH故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
设备是否为SSH服务器
查看SSH服务器状态
检查SSH服务器基本配置
查看密钥对
设置密钥对
检查客户端是否首次认证
检查SSH客户端配置
检查SSH服务器端公钥配置（Publickey认证）
检查客户端公钥（仅对Publickey认证）
拨打热线400-810-0504寻求帮助

06 安全产品 > 6.1 安全协议 > 6.1.4 SSH 故障排查 > 步骤详解

1. 开始

SSH 是 Secure Shell(安全外壳)的简称。用户通过一个不能保证安全的网络环境远程登录到设备时,SSH 可以利用加密和强大的认证功能提供安全保障,保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

设备既可以作为 SSH 服务器,又可以作为 SSH 客户端,所以排查故障的基本思路是:先判断设备是 SSH 客户端还是服务器,然后再检查设备基本配置,最后检查设备公钥和证书等信息。

2. 流程图相关操作说明

(1) 查看 SSH 服务器状态

如果设备作为 SSH 服务器,需要先查看 SSH 服务器是否使能。

命令:*display ssh server status*

例如:通过命令查看,可以确认设备已经使能 SSH 服务器。

```
<H3C>display ssh server status
 SSH server: Enable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP server Idle-Timeout: 10 minute(s)
```

(2) 检查 SSH 服务器基本配置

① 检查服务器的用户登录界面。SSH 客户端通过 VTY 用户界面访问设备。因此,需要配置 SSH 客户端登录时采用的 VTY 用户界面,使其支持 SSH 远程登录协议。配置结果在客户端下次请求登录时生效。

命令:*display current-configuration | begin vty*

例如:通过命令查看,可以确认是否配置了 VTY 认证方式、支持的协议以及访问命令级别,另外若是本地认证,毋忘添加本地用户。

```
<H3C>display current-configuration | begin vty
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
 protocol inbound ssh
```

② 检查用户服务类型和认证方式。检查用户的服务类型和认证方式是否正确。

命令:*display ssh user-information*

例如:通过命令查看,SSH 用户信息。

```
[H3C] display ssh user-information
 Total ssh users:1
Username            Authentication-type  User-public-key-name  Service-type
h3c                 password             null                  stelnet
```

(3) 检查密钥对

检查密钥对是否生成。虽然一个客户端只会采用 DSA 和 RSA 公钥算法中的一种来认证服务器,但由于不同客户端支持的公钥算法不同,建议在服务器上生成 DSA 和 RSA 两种密钥对。

命令: *display public-key local dsa/rsa public*

例如:通过命令查看,可以确认设备是否已经生成需要的密钥对。

```
<H3C>display public-key local dsa public
---------------------------------------------------
Time of Key pair created: 17:58:18   2013/05/06
Key name: HOST_KEY
Key type: DSA Encryption Key
---------------------------------------------------
Key code:
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44
…
<H3C>display public-key local rsa public
---------------------------------------------------
Time of Key pair created: 17:57:35   2013/05/06
Key name: HOST_KEY
Key type: RSA Encryption Key
---------------------------------------------------
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100A052FB39F578E44724A4EB
B201
…
---------------------------------------------------
Time of Key pair created: 17:57:40   2013/05/06
Key name: SERVER_KEY
Key type: RSA Encryption Key
---------------------------------------------------
Key code:
307C300D06092A864886F70D0101010500036B003068026100C7FDFDB
1E05E1D7846F5464A900B8418CF
…
```

(4) 设置密钥对

生成 RSA 密钥对时,将同时生成两个密钥对——服务器密钥对和主机密钥对;生成 DSA 密钥对时,只生成一个主机密钥对。

在检查和设置密钥对过程中,如果有密钥方面的问题,可以查阅相关云图或咨询技术客服。

命令: *public-key local create dsa/rsa*

```
[H3C]public-key local create dsa
The range of public key size is (512 ~ 2048).
```

```
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++++++++
[H3C]public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
+++++++++++++
```

(5) 检查客户端公钥(仅对 Publickey 认证)

Publickey 认证需要将客户端产生的公钥配置在服务器上,SSH 客户端使用 SSH 客户端软件生成 RSA 密钥对,将生成的 RSA 公钥保存到指定文件中,并将此公钥文件通过 FTP/TFTP 方式上传并导入到服务器,服务器可以通过命令查看是否存在登录客户端公钥。

命令:*display public-key peer brief*

例如:通过命令确认已经存在客户端的公钥对。

```
<H3C> display public-key peer brief
Type  Module  Name
---------------------------
RSA   1024    idrsa

DSA   1024    10.1.1.1
```

在服务器上检查客户端公钥配置,命令如下。

```
<H3C> display current-configuration | include public-key peer
public-key peerClient1 import sshkey 10.1.1.1
```

(6) 检查客户端是否首次认证

如果设备作为 SSH 客户端,先检查设备是否支持首次认证,如果支持首次认证,则当 SSH 客户端首次访问服务器,而客户端没有配置服务器端的主机公钥时,用户可以选择继续访问该服务器,并在客户端保存该主机公钥;当用户下次访问该服务器时,就以保存的主机公钥来认证该服务器。

如果不支持首次认证,则当客户端没有配置服务器端的主机公钥时,客户端将拒绝访问该服务器。用户必须事先将要访问的服务器端的主机公钥配置在本地,同时指定要连接的服务器端的主机公钥名称,以便客户端对连接的服务器进行认证。

命令:*undo client first-time*

ssh client first-time enable

例如:客户端支持首次认证,则可以直接与服务器建立连接。客户端不支持首次认证,则需要关闭客户端首次认证。若要开启,需要输入命令 ssh client first-time enable。

```
[H3C]undo ssh client first-time
[H3C]ssh client first-time enable
```

(7) 检查客户端配置

检查客户端是否配置服务器公钥并与服务器地址绑定。

命令：*display public-key peer*

display current-configuration | include ssh client authentication

例如：在公共密钥编辑视图输入服务器端的主机公钥，即在服务器端通过 display public-key local dsa public 命令显示的公钥内容，然后指定服务器对应的主机公钥名。

```
<H3C>display public-key peer
--------------------------------------
  Key Name   : key1
  Key Type   : DSA
  Key Module : 1024
--------------------------------------
Key Code:
308201B73082012C06072A8648CE3804013082...

<H3C>display current-configuration | include ssh client authentication
ssh client authentication server 10.1.1.1 assign publickey key1
```

(8) 检查 SSH 服务器端公钥配置(Publickey 认证)

若设备 SSH 作为客户端并且采用 Publickey 认证，需要生成本地密钥对，然后将生成的主机公钥导出到指定文件上传并导入到服务器。

命令：*display public-key local dsa public*

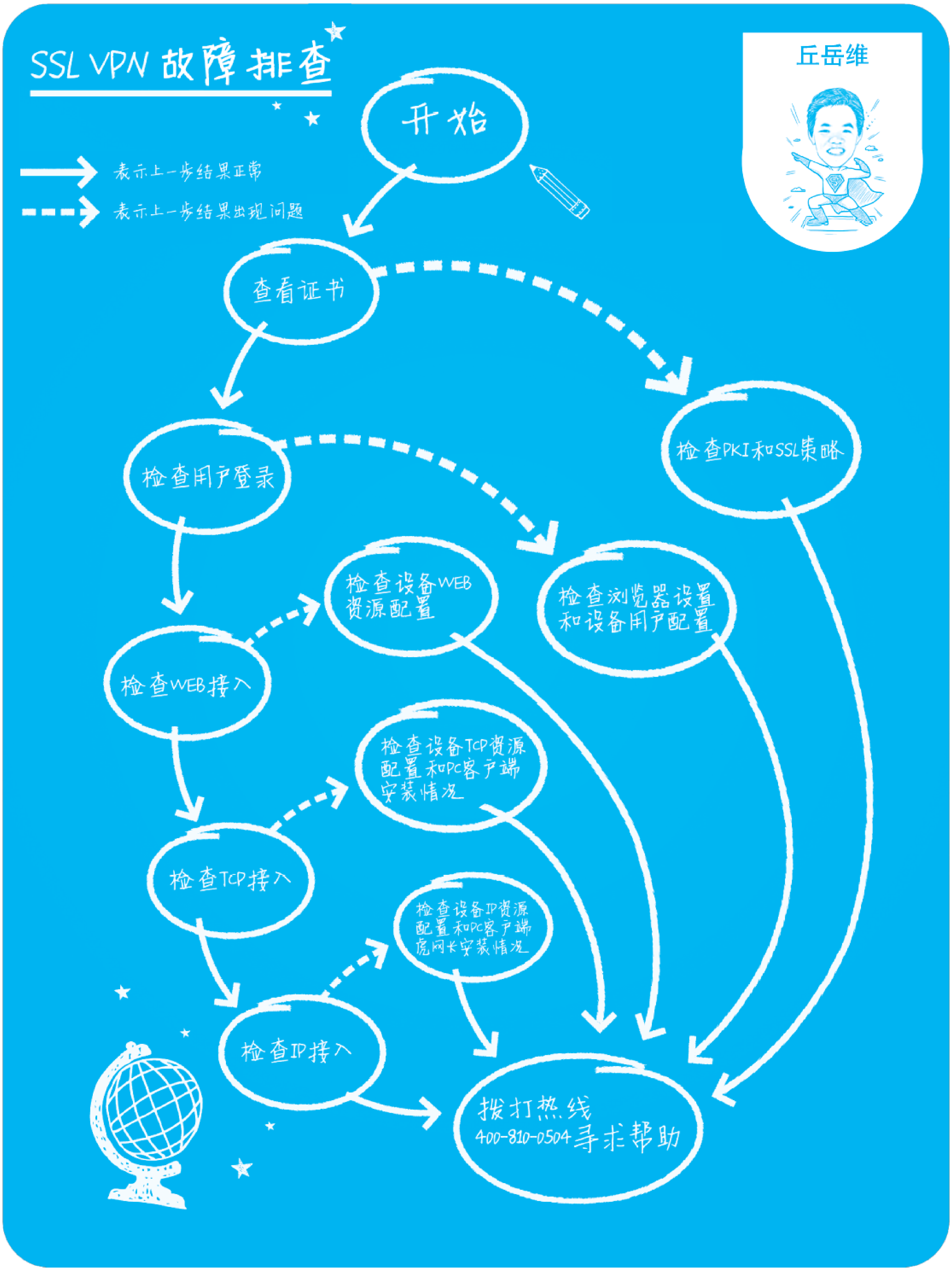
display current-configuration | include public-key peer

例如：在客户端生成公钥，public-key local create dsa，并将公钥导出到指定文件并上传到服务器上，同时在服务器配置 SSH 客户端公钥。

```
客户端上
<H3C>display public-key local dsa public
-----------------------------------------------------------
Time of Key pair created: 03:33:04  2013/06/24
Key name: HOST_KEY
Key type: DSA Encryption Key
-----------------------------------------------------------
Key code:
308201B83082012C06072A8648CE3804013082011F028181...

若要生成公钥文件,命令如下:
[H3C]public-key local export dsa ssh2 newkey

服务器上:
<H3C> display current-configuration | include public-key peer
public-key peer Client1 import sshkey newkey
```



SSL VPN 故障排查
丘岳维
表示上一步结果正常
表示上一步结果出现问题
开始
查看证书
检查PKI和SSL策略
检查用户登录
检查设备WEB资源配置
检查浏览器设置和设备用户配置
检查WEB接入
检查设备TCP资源配置和PC客户端安装情况
检查TCP接入
检查设备IP资源配置和PC客户端虚网卡安装情况
检查IP接入
拨打热线
400-810-0504寻求帮助

1. 开始

SSL VPN 是一种以 SSL 协议为基础的移动 VPN 技术，用户可以通过 Web、TCP 和 IP 三种方式接入 VPN 并访问内部网络资源。

SSL VPN 定位故障的思路是：先查看设备证书、PKI 以及 SSL 策略等配置是否正确，再查看 VPN 用户能否正常登录、VPN 客户端能否正常下载并安装，最后检查用户访问的特定资源是否正常。

2. 流程图相关操作说明

(1) 查看证书

分别查看是否存在 SSL VPN 相应 PKI 域的 CA 证书和 LOCAL 证书，且确认证书没有过期。

命令：*display pki certificate ca domain domain-name*

display pki certificate local domain domain-name

例如：通过命令查看，可以确认 svpndefdom 域的 CA 证书和 LOCAL 证书存在且没有过期。

```
<H3C>display pki certificate ca domain svpndefdom
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5814FC8D CE05DDB1 4C67DAA5 53D54BE2
...
        Validity
            Not Before: Apr 19 02:05:03 2013 GMT
            Not After : Apr 19 02:14:20 2018 GMT
...
<H3C>display pki certificate local domain svpndefdom
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            13604616 00000000 0011
...
        Validity
            Not Before: Apr 22 11:07:31 2013 GMT
            Not After : Apr 22 11:17:31 2014 GMT
...
```

(2) 检查 PKI 和 SSL 策略

SSL VPN 策略有服务器策略(必选)和客户端策略(可选)，在进行 SSL 服务器策略配置之前，还需要先配置 PKI 相关参数。先检查 PKI 域和实体的配置，然后检查 SSL 策略的配置。

命令：*pki domain domain-name*

pki entity entity-name

display web-server webserver-policy-name

display ssl server-policy sslserver-policy-name

display current-configuration | include svpn service

例如：通过命令查看 PKI 域和 SSL 策略的配置。

```
[H3C]pki domain svpndefdom
[H3C-pki-domain-svpndefdom]display this
#
pki domain svpndefdom
  ca identifier svpn
  certificate request entity svpndefent
  crl check disable
#
[H3C]pki entity svpndefent
[H3C-pki-entity-svpndefent]display this
#
pki entity svpndefent
  common-name svpn-gw
  organization-unit security
  organization h3c
  locality beijing
  state beijing
  country cn
#
<H3C>display web-server svpndefwsp
        Web server policy name: svpndefwsp
        Port:   443
        SSL server policy:   svpndefssp
        Debugging : off
        Operation status : Running
<H3C>display ssl server-policy svpndefssp
        ssl-policy: svpndefssp
        pki-domain: svpndefdom
        ciphersuite:
…
        session timeout: 3600
        session cachesize: 2000
        client-verify: weakenabled
        accelerator: use ssl-card 2/0
<H3C>display current-configuration | include svpn service
svpn service enable
```

(3) 检查用户登录

检查 VPN 用户的登录是否正常，能否获取到相应的 VPN 资源。

例如：登录普通 VPN 用户(Web-user)，可以正常获取到相应的资源，如图 6-5 所示。

(4) 检查设备配置和浏览器设置

检查设备上用户名、密码以及所属用户组配置是否正确，VPN 资源有没有添加到相应的



图 6-5 普通 VPN 用户登录

VPN 用户组。

例如：登录 VPN 管理员用户（administrator），查看用户所属的用户组以及关联的资源组，如图 6-6 所示。



图 6-6 VPN 管理员用户登录

检查浏览器的配置，ActiveX 控件是否正常下载并安装。确认浏览器的版本是否在 SSL 设备的支持范围内。

例如：IE 浏览器安全配置中对于 ActiveX 控件的推荐配置，如图 6-7 所示。



图 6-7 推荐配置

（5）检查设备 Web 资源配置

对于 Web 接入异常，主要是打开 Web 资源页面后，页面里有些链接打不开。需要检查这些链接是否链接到了别的服务器上，如果是，需要将该 Web 服务器也加入到 Web 资源里；若否，可将该链接网址加入到站点匹配模式中。

例如：Web 资源 www.h3c.com.cn 页面里有链接到其他网站 forum.h3c.com，那么就需要将后者也加入到 Web 资源里，如图 6-8 所示。



图 6-8　将链接网址加入站点匹配模式

（6）检查设备 TCP 资源配置和 PC 客户端安装情况

如果 TCP 接入异常，先检查 TCP 资源配置是否正确，用户组是否添加相应的 TCP 资源和 VPN 用户，再检查 VPN 客户端的安装以及本地监听端口是否正常。

例如：查看 TCP 资源配置正确，特别要注意端口和命令行的配置，如图 6-9 所示。



图 6-9　查看 TCP 资源配置

客户登录后查看 VPN 客户端已经安装并且端口监听正常，如图 6-10 所示。

（7）检查设备 IP 资源配置和 PC 客户端虚网卡安装情况

对于 IP 接入异常，先检查设备的 IP 网络中全局配置和主机配置，还要检查用户组是否添加相应的 IP 资源和 VPN 用户，再检查客户端虚拟网卡安装是否正常。

命令：*route print*

例如：查看设备的全局地址池配置，“网关地址”不能在“起始 IP”和“结束 IP”的范围内，如图 6-11 所示。

查看主机配置，添加了相应的 IP 资源，如图 6-12 所示。

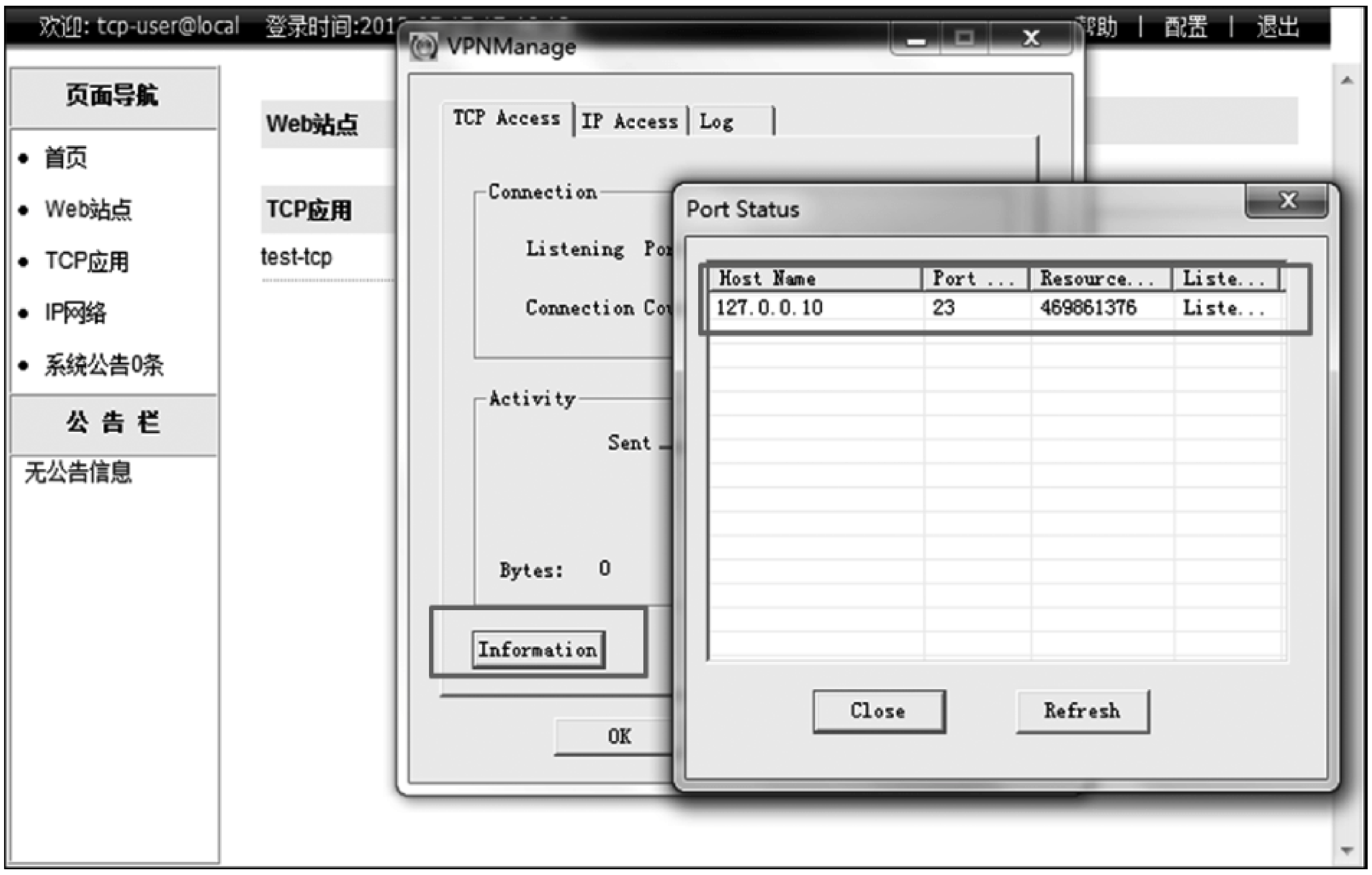


图 6-10 查看 VPN 客户端



图 6-11 设备全局地址池配置



图 6-12 主机配置

在客户端 PC 命令提示符(CMD)中分别输入 ipconfig /all 和 route print,可以看到 VPN 虚网卡、客户端获取的 IP 地址、SSL IP 地址池的路由和相应 IP 资源对应的路由。

```
C:\Users>ipconfig /all
以太网适配器 本地连接* 18:

    连接特定的 DNS 后缀 . . . . . . . :
    描述. . . . . . . . . . . . . . : SSLVPN Virtual Network Adapter(CS Support)
    物理地址. . . . . . . . . . . . . : 00-00-00-14-35-22
    DHCP 已启用. . . . . . . . . . . : 否
    自动配置已启用. . . . . . . . . . : 是
    本地链接 IPv6 地址. . . . . . . . : fe80::fd11:d374:f454:af7f%26(首选)
    IPv4 地址 . . . . . . . . . . . . : 10.0.0.5(首选)
    子网掩码 . . . . . . . . . . . . : 255.255.255.0
    默认网关 . . . . . . . . . . . . : 10.0.0.1
…
C:\\Users>route print
IPv4 路由表
-------------------------------------------------------------------------------------
活动路由:
网络目标        网络掩码          网关           接口          跃点数
0.0.0.0         0.0.0.0          192.168.0.1    192.168.0.2    276
10.0.0.0        255.255.255.0    在链路上        10.0.0.5       276
192.168.10.0    255.255.255.0    10.0.0.1       10.0.0.5       21
…
```


金 山
煎 饼
表示上一步结果正常
表示上一步结果出现问题
开始
公钥管理故障排查
检查本地
非对称密钥
检查远端主
机公钥信息
创建本地
非对称密钥对
配置远端主机
公钥信息
拨打热线
400-810-0504寻求帮助

1. 开始

公钥问题定位故障的思路是：查看本地是否创建生成了符合要求的非对称密钥对，对于需要使用远端主机公钥的，还需要进一步排查预先配置的远端主机公钥信息是否正确。

2. 流程图相关操作说明

(1) 检查本地非对称密钥对

查看本端设备当前是否存在本地 RSA/DSA 密钥对。

命令：*display public-key local rsa public*

display public-key local dsa public

若执行命令后，命令行界面上无任何对应输出，则说明系统当前没有生成相应的非对称密钥对。

例如：通过命令查看当前设备的 RSA 密钥对。

```
<H3C>display public-key local rsa public
--------------------------------------------------------------------------------
Time of Key pair created: 03:11:19   2013/05/02
Key name: HOST_KEY
Key type: RSA Encryption Key
--------------------------------------------------------------------------------
Key code:
…
--------------------------------------------------------------------------------
Time of Key pair created: 03:11:21   2013/05/02
Key name: SERVER_KEY
Key type: RSA Encryption Key
--------------------------------------------------------------------------------
Key code:
…
```

(2) 检查远程主机公钥信息

查看本端是否正确配置了远程主机的公钥信息。

命令：*display public-key peer name xxx*

例如：通过命令查看当前系统中配置的名称为“rsa_peer_a”的远程主机其 RSA 公钥。

```
<H3C> display public-key peer name rsa_peer_a
------------------------------
  Key Name   : rsa_peer_a
  Key Type   : RSA
  Key Module: 1024
------------------------------
Key Code:
…
```

(3) 创建本地非对称密钥对

当系统中尚未创建本地密钥对时，可以直接在设备上通过命令创建。

当出现如下几种情况时，也需要重新生成新的本地密钥对。

① 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。

② 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加/解密和数字签名。

③ 密钥对使用了较长时间，可能存在密钥泄露或破译的风险。

④ 本地证书到达有效期，需要删除对应的本地密钥对。

命令：*public-key local create rsa*

public-key local create dsa

例如：通过命令创建模数长度为2048位的RSA公私钥对。

```
[H3C] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]: 2048
Generating Keys...
+++
++++++++++++++++++++++++++++++
+++++++
++++++
```

(4) 配置远程主机公钥信息

当系统其他软件模块需要提前知晓相关远程主机的非对称密钥公钥信息时，需预先配置其公钥信息。

配置远端主机公钥的方式有如下两种。

① 从公钥文件中导入。首先将远端主机的公钥文件保存到本地设备(注意，通过FTP或TFTP方式传输文件时，必须以二进制方式将远端主机的公钥文件保存到本地设备)，然后从该公钥文件中导入远端主机的公钥。导入公钥时，系统会自动将远端主机的公钥文件转换为PKCS(Public Key Cryptography Standards，公共密钥加密标准)编码形式。

② 手工配置。首先在远端主机上查看其公钥信息，并记录远端主机公钥的内容。然后在本地设备上采用手工输入的方式将远端主机的公钥配置到本地。手工输入远端主机公钥时，可以逐个字符输入，也可以一次复制粘贴多个字符。

命令：*public-key local export rsa { openssh | ssh1 | ssh2 } xxx*

public-key peer xxx import sshkey xxx

例如：通过命令将远程主机的公钥信息导出至文件，然后通过文件导入至本地设备。

```
[Remote_Device] public-key local export rsa ssh2 key.pub

[H3C] public-key peer remote_device import sshkey key.pub
```

命令：*public-key peer xxx*

例如：通过命令配置名称为"rsa_peer_a"的远程主机公钥信息。

```
[H3C] public-key peer rsa_peer_a
Public key view: return to System View with "peer-public-key end".
```

```
[H3C-pkey-public-key] public-key-code begin
Public key code view: return to last view with "public-key-code end".
[H3C-pkey-key-code] 30819F300D06092A864886F70D010101050003818D00308189028181
00D90003FA95F5A44A2A2CD3F814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162
D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784AD597D0FB3AA9F7202C507072B19C
3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80AAB5EE01986BD1E
F64B42F17CCAE4A77F1EF999B2BF9C4A10203010001        //注意此处公钥仅为示例
[H3C-pkey-key-code] public-key-code end
[H3C-pkey-public-key] peer-public-key end
```



沈博文
ACG1000c 微信认证故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看微信自动回复
检查微信公众号配置
检查用户认证配置
检查设备策略配置
查看在线用户状态
检查微信认证配置
拨打热线
400-810-0504
寻求帮助

1. 开始

微信认证是 ACG1000 的重要功能之一。微信认证不仅仅需要在 ACG1000 设备上进行配置,还需要微信公众平台或者第三方运营平台的配合。ACG1000 微信认证故障定位的思路是:首先确认微信公众号可以正确自动回复所设定的链接,其次检查用户认证的配置,再次查看设备是否默认放通了微信流量,最后确认设备上微信认证的配置是否正确。

2. 流程图相关操作说明

(1) 查看微信自动回复

通过移动终端连接到需要微信认证的 WIFI 网络中,客户端直接访问网页时,会跳转至导航页面,无法上网。用户需要通过微信二维码等方式关注相应公众号后,通过发送关键字到公众号,并且单击公众号的回复内容后,即可上网。所以第一步需要查看公众号是否可以完成自动回复,并且要求自动回复的链接是实际可以打开的网络链接,这里建议微信公众号设置自动回复的跳转页面链接为动态页面,如果跳转页面使用静态页面,则可能由于缓存导致认证失败,此时需要清空客户端网页缓存。

(2) 检查微信公众号配置

如果微信公众号平台不能自动回复网络链接,那么需要排查微信公众号平台配置,正确配置如下,请核对检查。

① 登录微信公众平台。如图 6-13 所示,登录微信公众平台 https://mp.weixin.qq.com/,输入注册的用户名和密码,单击“登录”按钮。



图 6-13 登录微信公众平台

② 编辑模式配置(与开发者模式二选一即可)。如图 6-14 所示,在公众平台配置界面单击“自动回复”按钮,并单击“开启”按钮。

如图 6-15 所示,单击“关键字自动回复”按钮,并单击“添加规则”按钮进入新规则编辑页面,“规则名”配置为“微信认证”,“关键字”添加为 test,“回复”配置为“点击上网”,注意此处配置的 URL 不支持 HTTPS 链接,仅支持 HTTP 链接。(更多关键字规则配置请参考微信公众平台帮助文档。)



图 6-14　开启自动回复功能



图 6-15　编辑模式下添加自动回复

③ 开发者模式配置(与编辑者模式二选一即可)。

如图 6-16 所示,单击“开发者中心”选项,在页面中选择“启用”选项,单击“确认”按钮后,填写从第三方运营平台获取的 URL 和 Token。(更多配置请参考微信公众平台开发者文档。)

如图 6-17 所示,进入第三方公众号运营平台进行配置。(这里使用 www. uip. cn 为例,各个平台虽有差异但配置较为统一。)

如图 6-18 所示,单击“文本回复”选项,“关键词”配置为 test,“内容或简介”配置为“我要上网”,注意此处配置的 URL 不支持 HTTPS 链接,仅支持 HTTP 链接。

以上为微信公众平台正确配置。

(3) 查看在线用户状态

点击微信公众平台自动回复的链接,打开所设置网页的界面以后,用户即可正常上网,如



图 6-16　启用开发者模式



图 6-17　第三方公众号运营平台配置页面



图 6-18　第三方公众号自动回复内容设置

果此时不能正常上网，需要在 ACG1000 管理界面上查看在线用户状态，确认此用户是否认证成功，如图 6-19 所示。



图 6-19　查看在线用户状态

(4) 检查用户认证配置

如果在上一步中未查看到用户在线，那么说明此用户没有认证成功，首先需要确认设备上用户认证的配置是否正确。

在 ACG1000 管理界面，单击“用户管理”→“用户”命令，查看是否配置了用户，若未配置用户，请使用如下方法添加本地用户进行测试。

单击“新建”按钮，用户命名为 test，“认证方式”选择“本地认证”单选按钮，输入并确认密码，选中“启用”复选框，单击“提交”按钮，如图 6-20 所示。

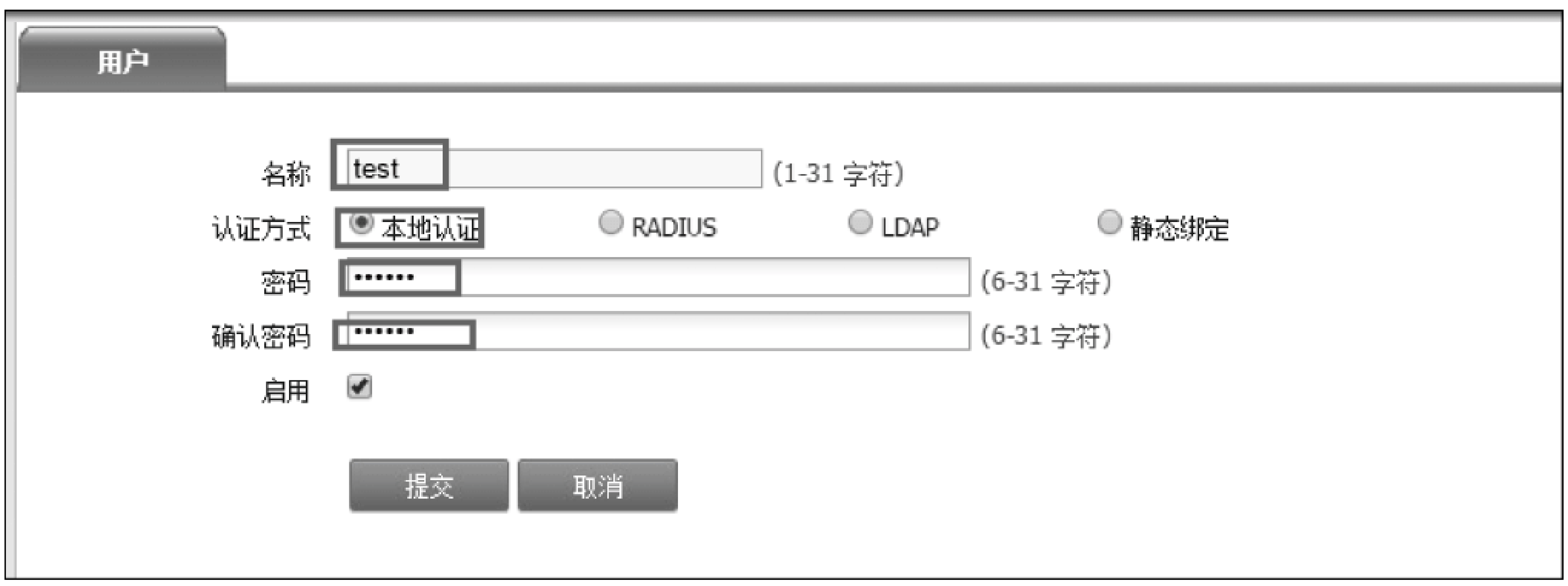


图 6-20　添加本地认证用户

(5) 检查设备策略配置

ACG1000 配置微信认证时，设备需要默认放通微信流量，请检查设备是否配置放通微信流量的策略，单击“上网行为管理”→“策略配置”→“IPv4 策略”命令，配置如图 6-21 所示。



图 6-21　IPv4 策略配置

（6）检查微信认证配置

确认以上配置无误后，最后需要确认设备微信认证配置是否正确，单击“用户管理”→“认证服务器”→“微信认证”命令，确认“微信认证弹出 URL”配置为 www.xxx.com（和微信公众平台配置保持一致），选中“启用”复选框，选中“超时时间”复选框，并配置“超时时间”，“源地址”配置为允许进行微信认证的地址对象，其他配置保持默认，如图 6-22 所示。

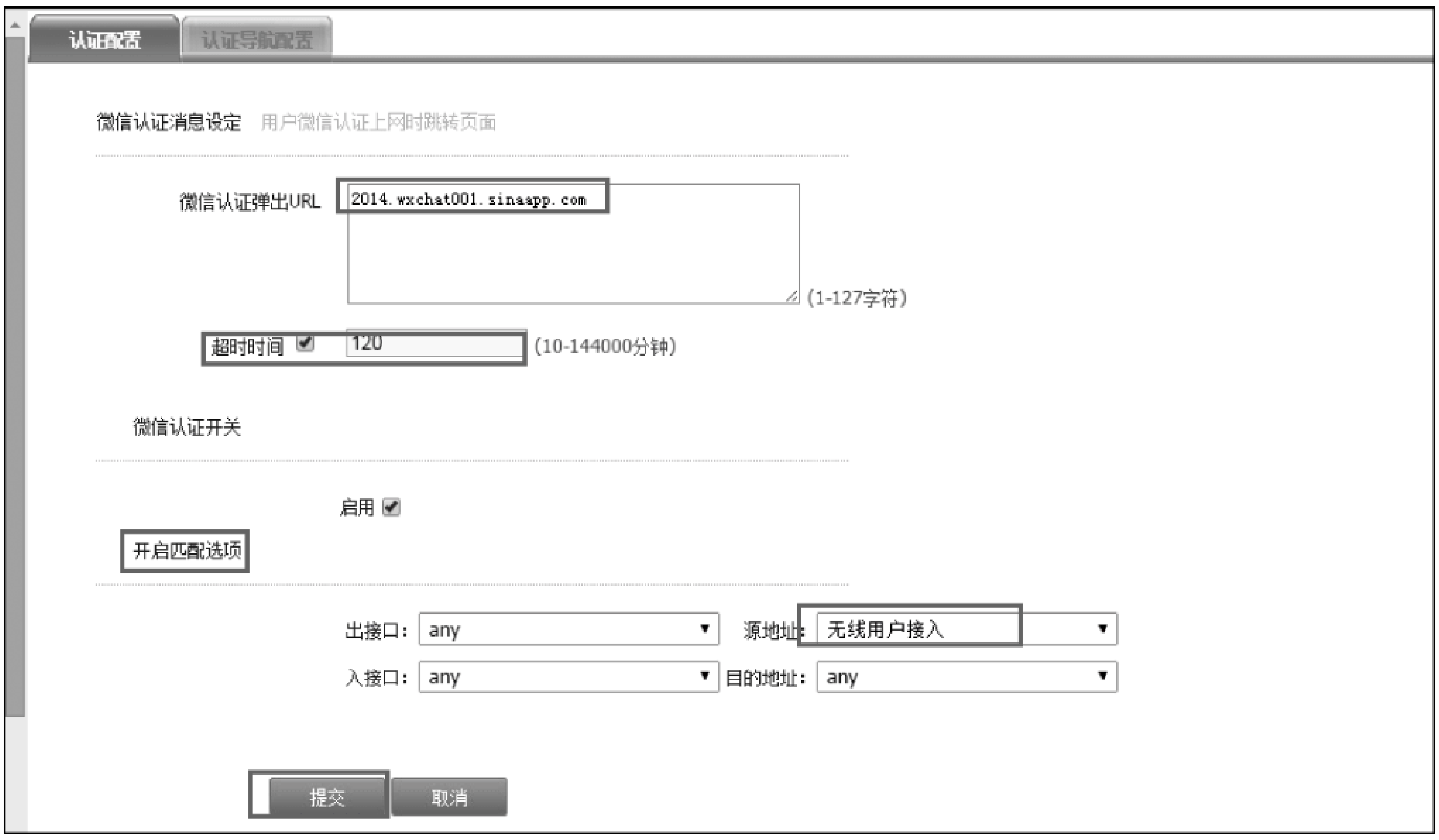
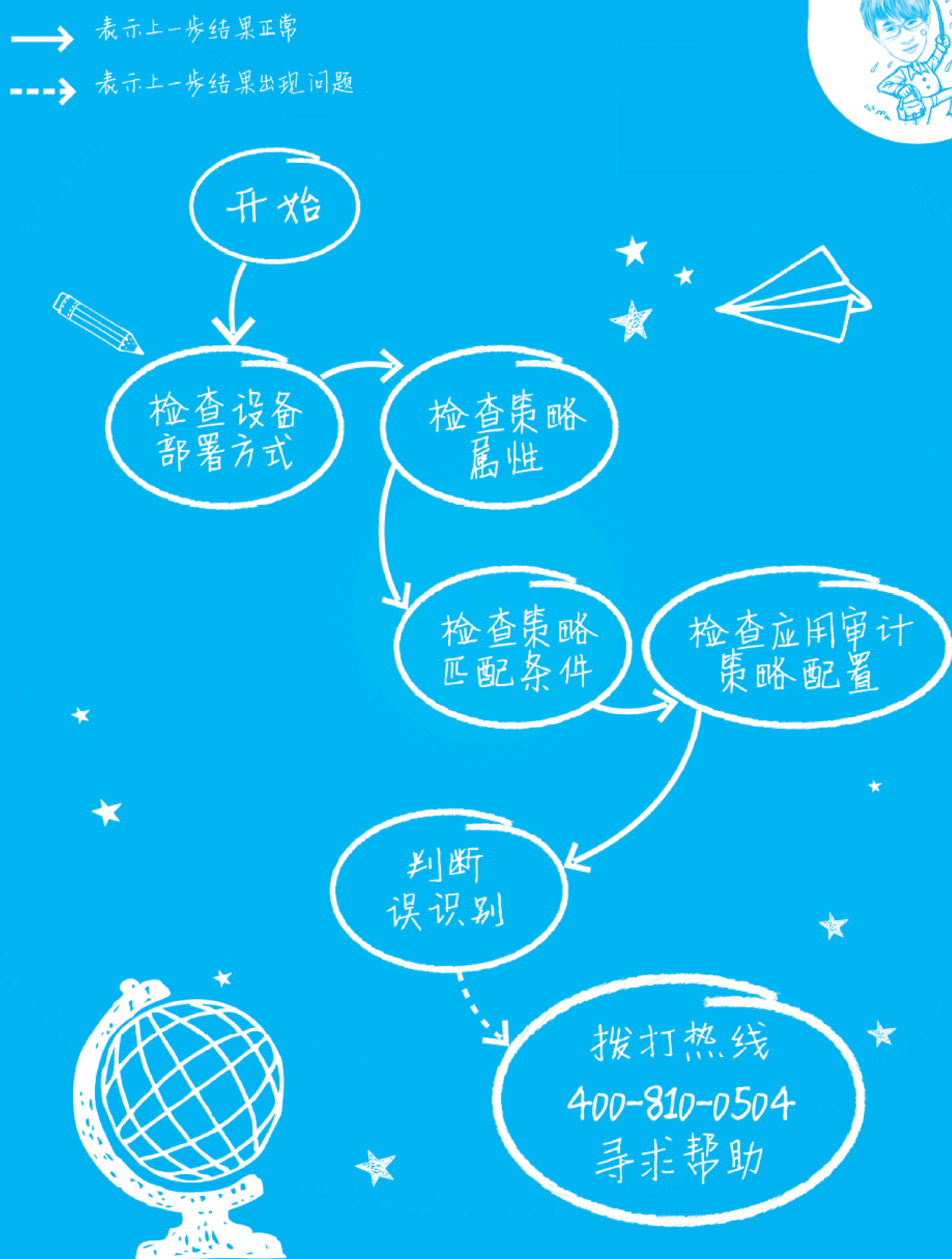


图 6-22 微信认证配置

ACG1000应用审计功能故障排查

莘启跃





1. 开始

ACG1000 应用审计功能可对各种网络社区、P2P/IM、网络游戏、网络多媒体、文件共享、邮件收发、数据传输、数据库应用等各种上网行为提供全方面的行为监控和记录；同时，通过综合分析、检测用户网络流量与流向趋势，对历史数据进行分析，为用户提供细粒度的网络应用审计管理。

ACG1000 应用审计功能故障的定位思路是：首先明确设备的部署方式，确认用户流量是否命中策略，其次判断是否有应用存在误识别的情况，对于应用误识别问题，收集相关信息反馈。

2. 流程图相关操作说明

(1) 检查设备部署方式

ACG1000 分为在线部署和旁路部署。在线部署方式使得 ACG1000 能够串接在网络中，用户流量直接经过设备，设备能够对应用进行监控和管理，保障关键应用和服务的带宽。采用旁路部署时，ACG1000 旁挂在核心设备旁，用户的流量通过镜像方式上送至 ACG1000 进行审计，而无法对上网行为进行干预，如放行或阻断。

在线部署拓扑图，如图 6-23 所示。

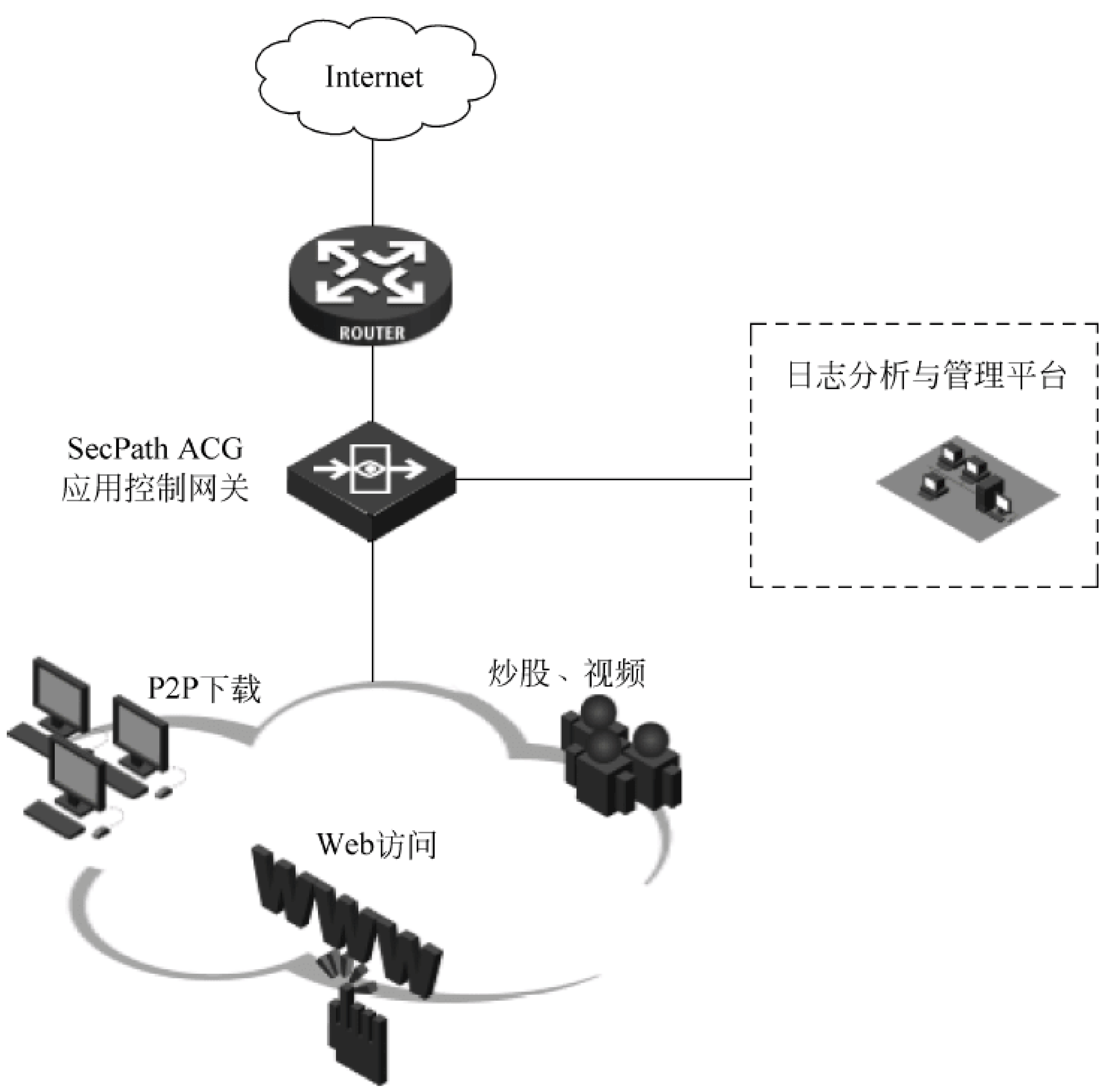


图 6-23　在线部署拓扑

旁路部署拓扑图，如图 6-24 所示。

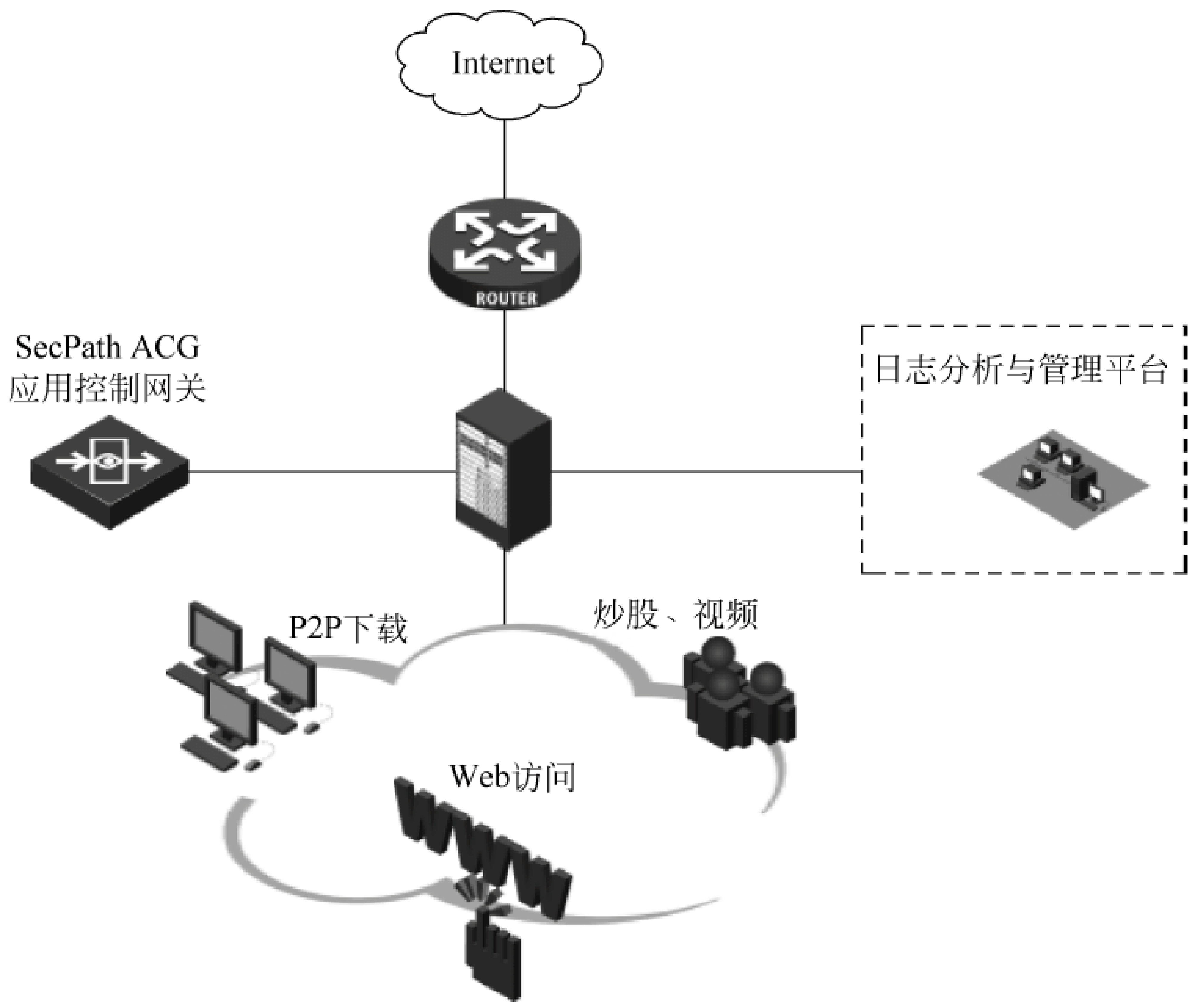


图 6-24　旁路部署拓扑

登录 ACG1000 Web 管理界面，查看设备目前的部署方式，如需设备参与用户上网行为允许或阻断，则应关闭旁路部署。

例如：通过 Web 页面查看 ACG1000 当前部署方式，路径为“系统管理→部署方式”，如图 6-25 所示。

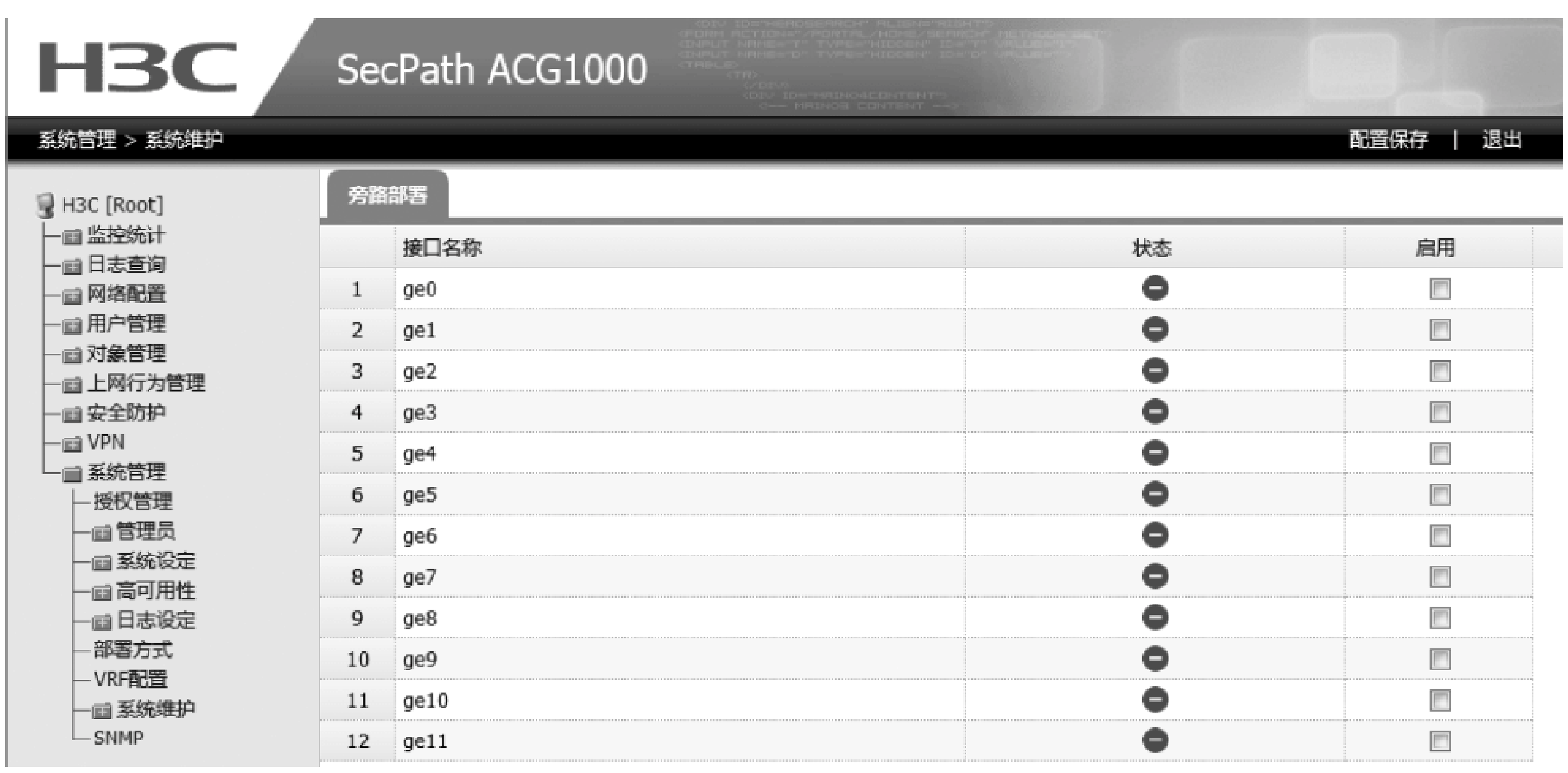


图 6-25　ACG1000 当前部署方式

登录 Web 界面，可以看到接口并未启用旁路部署，在此情况下，ACG1000 才能对用户上网行为进行允许或阻断，否则只能进行审计。

(2) 检查策略属性

检查策略属性需同时关注启用状态及动作类型。

① 检查应用审计策略是否启用,若未启用则无法对用户上网行为进行审计。例如:通过Web页面查看ACG1000应用审计策略是否启用,路径为"上网行为管理→策略配置→IPv4策略/IPv6策略→状态",如图6-26所示。



图 6-26 检查策略属性

当状态一栏显示为 ✔,表明应用审计策略启用。

② 检查策略动作。策略属性中的动作分为审计、免审计、拒绝,当动作为审计时才能对用户上网行为进行审计。

例如:通过Web页面查看ACG1000应用审计策略动作是否为审计,路径为"上网行为管理→策略配置→IPv4策略/IPv6策略",如图6-27所示。



图 6-27 检查策略动作

当显示为 ■▷,表明应用审计策略动作为审计。

(3) 检查策略匹配条件

在策略匹配条件中,可调用用户、源接口/域、目的接口/域、源地址、目的地址、时间、服务,这些参数既可以预定义又可自定义。

例如:通过Web界面查看ACG1000应用审计策略匹配条件的配置,路径为"上网行为管理→策略配置→IPv4策略/IPv6策略"。单击操作中的"编辑"按钮可进行修改,如图6-28和图6-29所示。



图 6-28 检查策略匹配条件



图 6-29 修改策略匹配条件

(4) 检查应用审计策略配置

检查应用审计策略配置时，应关注匹配选项。匹配选项包括全匹配和顺序匹配，其中，全匹配表示同一数据包自上而下匹配全部策略，如命中阻断策略数据包丢弃；顺序匹配表示同一数据包自上而下仅匹配到首次命中的策略。

例如：通过 Web 界面查看 ACG1000 应用审计策略匹配选项的配置，路径为“上网行为管理→策略配置→IPv4 策略/IPv6 策略→操作(编辑)→应用策略→匹配选项”，如图 6-30 所示。

由于迅雷/迅雷看看均为迅雷旗下应用，两者共用了 P2P 下载引擎的相关技术，因此迅雷在下载某些特定资源时，会通过迅雷看看的资源进行获取；同样的，迅雷看看的某些特定资源也会从迅雷资源获取。因此，这两款软件会出现一些误报，基于类似的原因 QQ 旋风和腾讯视频也会出现一些误报。如果需要进行流控/阻断，建议将两个应用一起选择。



图 6-30 检查应用审计策略配置

(5) 判断误识别

① 通过 Web 页面流量监控情况判断。ACG1000 的 Web 界面中可实时查看系统目前使用流量最大的 top 应用，粗略判断应用是否误识别。路径："监控统计→系统状态→应用流量排名"，如图 6-31 所示。

应用流量排名

	应用类型	上行	下行	总流速	百分比
1	同花顺	136.80 (b/s)	141.60 (b/s)	278.40 (b/s)	56.12 %
2	域名解析协议(DNS)	52.00 (b/s)	165.60 (b/s)	217.60 (b/s)	43.87 %

图 6-31 应用流量排名

此时如果想要限制 HTTP 协议而没有限制成功，却发现系统上同花顺应用的流量很大，则可以推断 HTTP 协议被误识别为了同花顺协议。

② 通过查看会话判断。使用 display ip connection protocol 查看特定会话，关注会话中的 AppName 字段，确认是否被误识别为其他应用。

命令：*display ip connection protocol* [*protocol-name*] *ip source* [*source-addr*] *dest* [*dest-addr*]

例如：在命令行下查看源地址为 10.8.3.22 的会话。

```
ACG1000> en
ACG1000# display ip connection protocol all ip source 10.8.3.22 dest any
matched connection count: 90
Protocol:   UDP State:Complete      PolicyID:1         VrfId:0
                Status: 0x0062409e                 FastCode: 0x0000033f
```

```
                    UserName:x10216                    AppName: HTTP
                    Expire: 00:00:58                   Existed: 00:10:53
                    Source Dir: 10.8.3.22:51742      > 183.60.56.19:8021
                    Reply   Dir: 183.60.56.19:8021   > 60.191.123.71:51742
Protocol:   TCP State:Complete      PolicyID:1       VrfId:0
                    Status: 0x0062c09e                 FastCode: 0x0000037f
                    UserName:x10216                    AppName: HTTP
                    Expire: 00:59:50                   Existed: 00:15:40
                    Source Dir: 10.8.3.22:61846      > 122.225.207.219:5061
                    Reply   Dir: 122.225.207.219:5061 > 60.191.123.71:61846
                    This connection has SRC_NAT
Protocol:   TCP State:Halfopen      PolicyID:1       VrfId:0
                    Status: 0x00226098                 FastCode: 0x0000013f
                    UserName:x10216                    AppName: HTTP
                    Expire: 00:00:02                   Existed: 00:00:26
                    Source Dir: 10.8.3.22:62292      > 74.125.23.113:80
                    Reply   Dir: 74.125.23.113:80    > 60.191.123.71:62292
                    This connection has SRC_NAT
```

假如 10.8.3.22 这台主机的迅雷无法被限制的时候，通过会话查看 AppName 字段都识别为 HTTP，则可以推断迅雷应用被误识别为 HTTP 应用。

③ 通过 debug 方式。在 ACG1000 设备上配置 debug application identify 和 debug app audit detail 可打印出应用识别和审计的细节，使用 show log debug 加具体协议名字查看 debug 信息。

命令：*debug application identify*

debug app audit detail

display log debug [*FILTER*]

例如：在命令行下通过 debug 信息可以看到 HTTP 协议被 app policy 1 识别出，审计时记录了网页浏览的日志。

```
ACG1000> en
ACG1000# debug application identify
ACG1000# debug app audit detail
ACG1000#display log debug HTTP
<15>Jun 21 13:35:03 dplane: Match the app policy 1 app_id HTTP action: permit
<15>Jun 21 13:35:22 dplane: ident as application HTTP(#4085) Web_access(#76) HTTP_RULE_
2(#0xffffc9)
<15>Jun 21 13:35:22 dplane: set packet high protocol HTTP(#9)
<15>Jun 21 13:35:22 dplane: Match the app policy 1 app_id HTTP action: permit
<15>Jun 21 13:35:22 dplane: Audit other_app log to syslog:user_id=2;user_name=172.30.1.13;
user_group_id=2;user_group_name=anonymous;term_platform=windows;term_system=;term_
device=;term_supplier=;src_ip=172.30.1.13;dst_ip=42.121.1.101;dst_port=80;ip_version=0;
app_id=2147487733;app_name=网页浏览(HTTP);app_cat_id=11534336;app_cat_name=网络协
议;character_id=0;character_name=accept;level_id=6;level_name=info;service=0;account=;
action_id=76;action_name=Web浏览;create_time=
        Audit other_app log to database:2,"172.30.1.13",2,"anonymous","windows","","","",
"172.30.1.13","42.121.1.101",80,0,2147487733,"网页浏览(HTTP)",11534336,"网络协议",0,
"accept",6,"info",0,"",76,"Web浏览"4
```

如 display log debug HTTP 无打印，则证明没有识别出 HTTP。

④ 信息收集。

(a) 导出设备的配置文件。路径为“系统管理→配置文件→导出配置→导出”,如图 6-32 所示。



图 6-32 导出设备配置文件

(b) 导出设备的诊断信息。路径为“系统管理→信息收集→收集→提交→操作(下载)”,如图 6-33 所示。

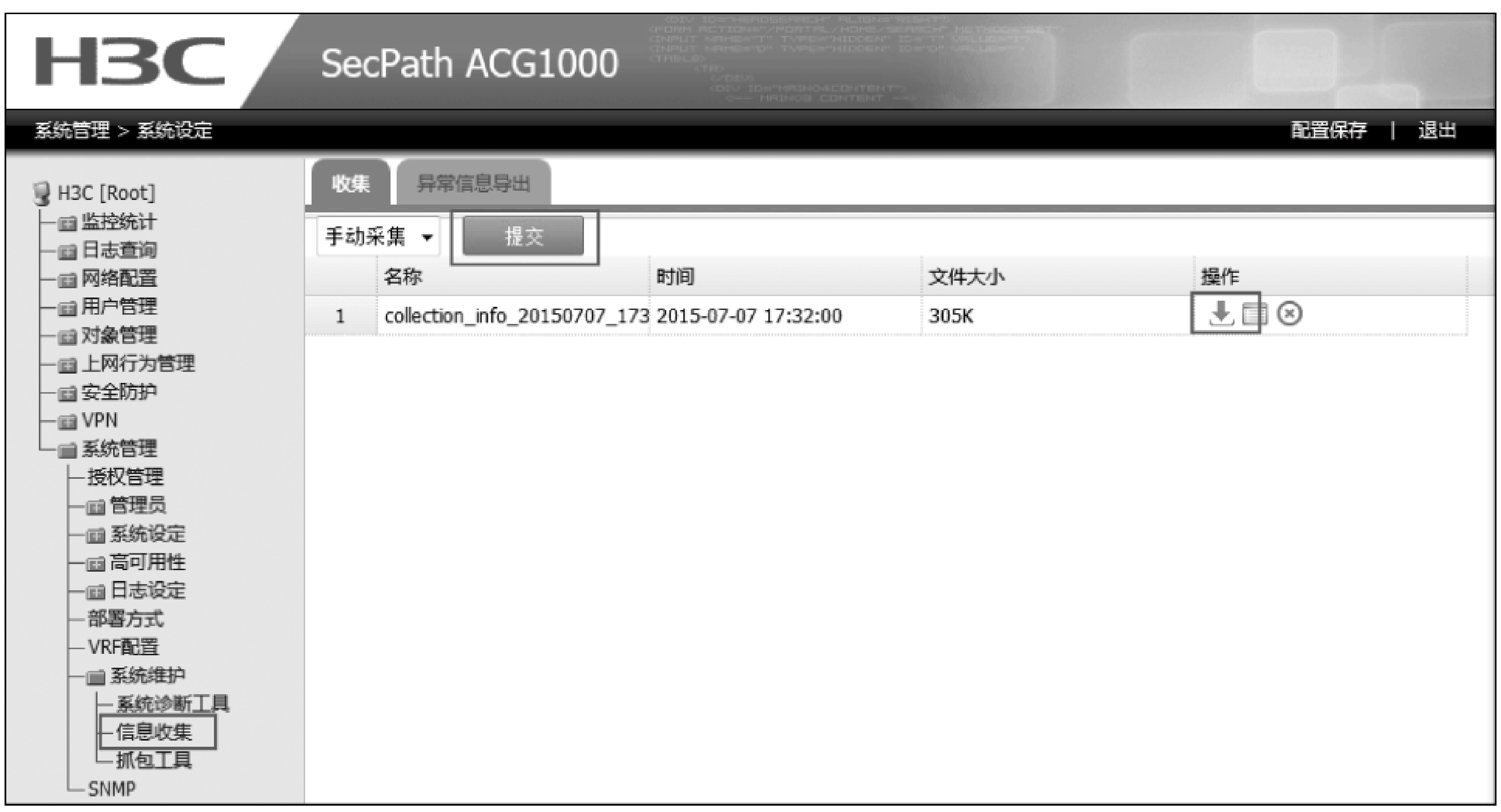


图 6-33 导出设备诊断信息

(c) 导出设备的异常信息(如果有)。路径为“系统管理→信息收集→异常信息导出→操作(下载)”,如图 6-34 所示。

(d) 抓取应用报文。ACG1000 自带抓包工具,可以定义相关参数抓取故障时的报文,如图 6-35 所示。

(e) 记录反馈前期所有的操作。



图 6-34　导出设备异常信息



图 6-35　抓取应用报文



ACG1000 URL功能问题故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
检查设备状态
检查接口状态
检查用户状态
检查部署方式
是否启用自定义URL过滤
检查自定义URL配置
检查策略配置
检查地址对象配置
检查时间表配置
检查访问网站日志
拨打热线
400-810-0504
寻求帮助

1. 开始

ACG1000 URL 功能问题定位故障的思路是：①检查设备系统状态、接口状态是否正常；②检查用户状态是否正常上线；③检查设备部署方式是否合理；④依次检查自定义 URL 配置(若启用自定义 URL 过滤)、策略配置、地址对象配置、时间表配置是否正常；⑤检查访问网站日志是否有对应的日志信息输出。在排查过程中，还需要注意客户端侧的 DNS 解析是否正确，浏览器工作是否正常，排除客户端浏览器或 Web 网站故障引起的问题。

2. 流程图相关操作说明

(1) 检查设备状态

进行 URL 功能问题排查时，首先确认当前设备运行状态是否正常，是否出现 CPU、MEM 过载问题。如果发现系统运行状态值异常，建议转其他相关问题的云图继续排查，待系统运行状态恢复后再进行 URL 功能问题排查操作。

命令：无

例如：在 ACG Web 管理界面单击“监控统计”→“系统状态”命令，检查“系统资源”运行参数是否正常，如图 6-36 所示。

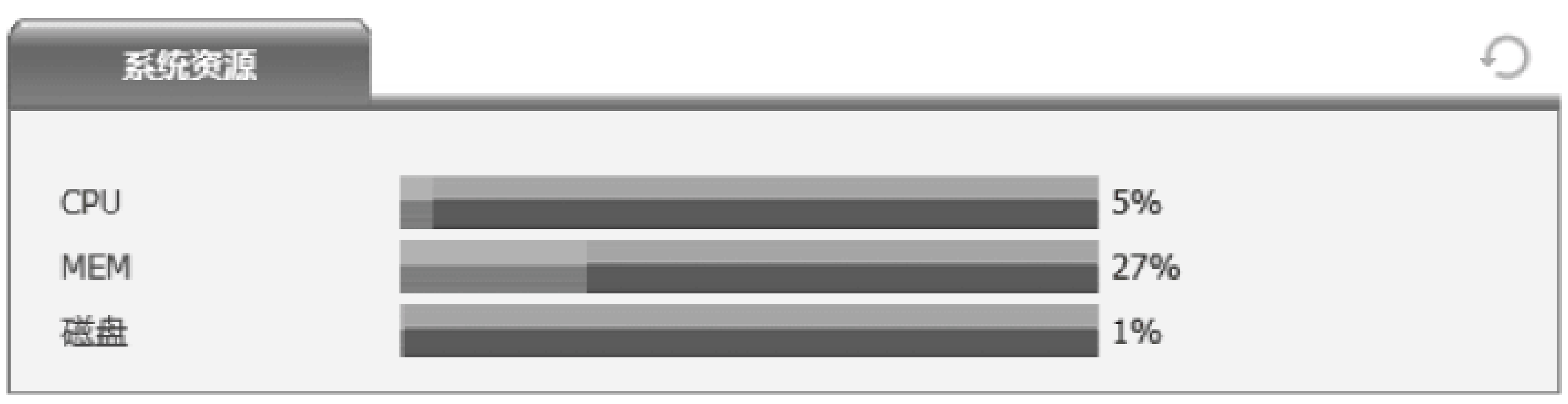


图 6-36　系统资源

例如：在 ACG Web 管理界面单击“监控统计”→“系统状态”命令，检查“实时流量”运行统计值是否正常，是否符合日常运维观察到的数值范围，如图 6-37 所示。若实时流量出现较大的突发，则可能是网络中存在异常流量，建议根据入接口及上下行统计值信息，进一步做排查，判断是否存在主机中病毒或存在网络攻击，导致对网络设备产生冲击。

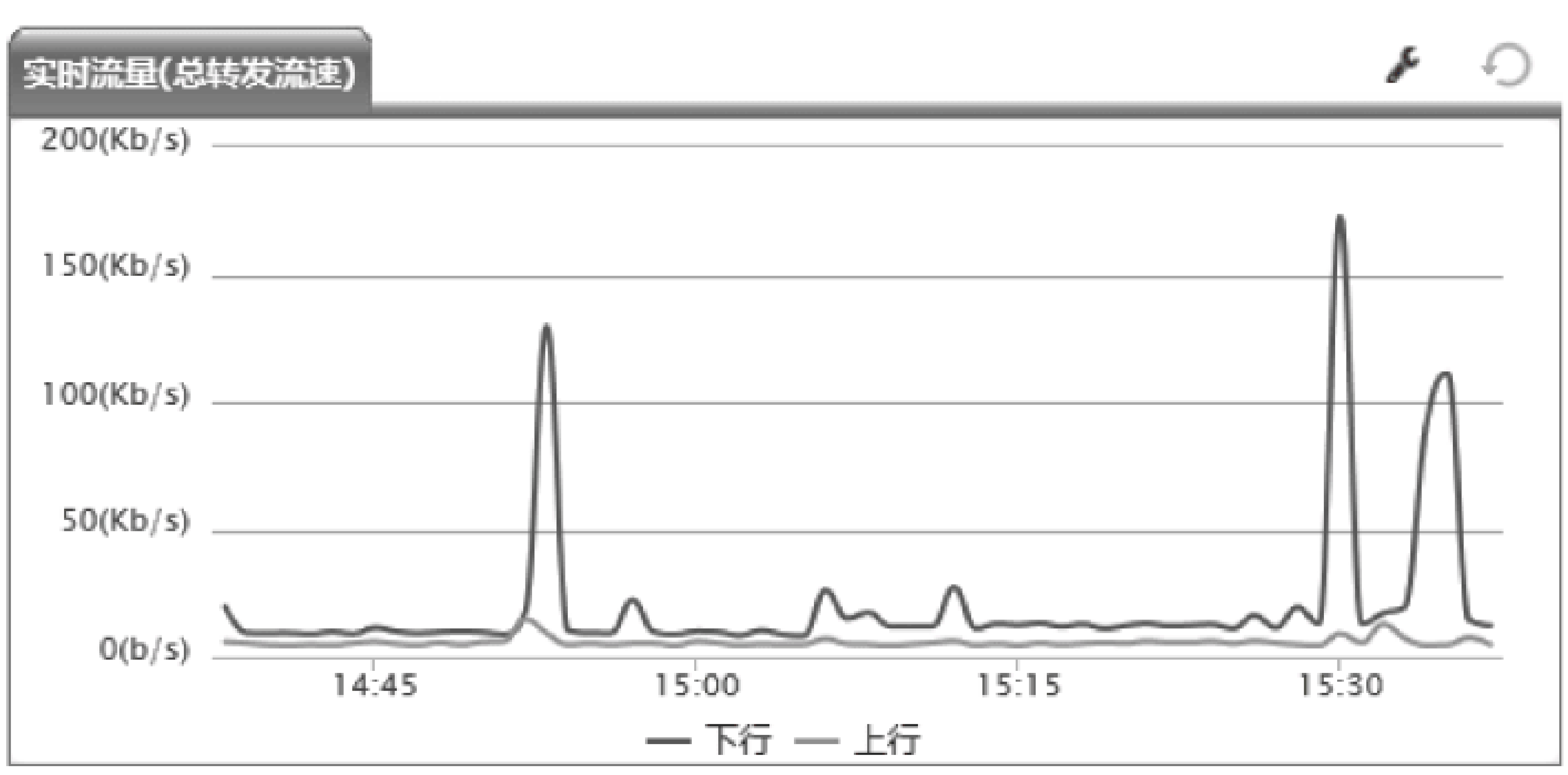


图 6-37　实时流量

(2) 检查接口状态

检查 ACG 设备接口状态即工作速率、双工模式是否正常,接口报文收发速率是否与业务流量情况相符,特别要注意接口的物理连线是否与配置预期相符。

命令:无

例如:在 ACG Web 管理界面单击"监控统计"→"接口状态"命令,检查相关接口状态是否正常,如图 6-38 所示。重点检查"链路状态""工作速率""双工模式""接收速率""发送速率"等项目的状态是否正常,是否符合实际网络情况。当启用 ACG 二层透明部署时,还需根据"属性"字段检查 ACG 设备上下行物理端口是否处于同一个 BVI 桥接组中。特别地,强烈建议现场工程师到设备旁仔细核对设备上的物理连线是否正确,是否符合物理组网拓扑规划。

接口状态

清除计数

	名称	链路状态	属性	工作速率	双工模式	IP地址	IPv6地址	接收速率	发送速率
1	ge0	-	-	1000	full	172.31.0.2/24		0 bps	0 bps
2	ge1	-	-	1000	full			0 bps	0 bps
3	ge2	up	bvi1	100	full			9.72 Kbps	4.47 Kbps
4	ge3	up	bvi1	1000	full			10.05 Kbps	10.20 Kbps
5	ge4	-	-	1000	full			0 bps	0 bps
6	ge5	-	bvi0	1000	full			0 bps	0 bps
7	ge6	-	-	1000	full			0 bps	0 bps
8	ge7	-	-	1000	full			0 bps	0 bps
9	ge8	up	bvi0	1000	full			0 bps	0 bps
10	ge9	-	-	1000	full			0 bps	0 bps

图 6-38 接口状态

(3) 检查用户状态

ACG 设备支持用户认证功能,若配置启用了相关特性,在排查 URL 功能前需检查客户端用户在设备上是否已经通过认证,是否可以通过 ACG 设备访问网络资源。默认配置情况下,ACG 设备未启用认证,最终用户通过 ACG 设备可以任意访问网络,此时该最终用户属于"匿名用户组"。若设备启用了本地或第三方认证,或最终用户需要通过其他设备进行接入认证,则需要检查认证是否完成。若认证未通过,用户未能成功上线,则需要先排除认证相关问题。

命令:无

例如:在 ACG Web 管理界面单击"监控统计"→"在线用户管理"命令,检查"在线用户管理"或"移动用户管理"中的用户在线情况是否正常。在如图 6-39 所示,IP 地址为 10.88.8.115 的用户未在 ACG 上启用认证,其状态为"正常",若网络中不存在其他设备执行接入认证,则该用户可以正常通过本 ACG 设备访问网络。

(4) 检查部署方式

ACG 设备支持"在线"或"旁路"两种部署方式。当工作在"在线"模式时,支持阻断动作并产生日志;当工作在"旁路"模式时,仅支持日志审计功能,无法执行 URL 阻断过滤动作,因此需要根据客户部署需求,检查设备工作模式是否配置合理。

命令:无

例如:在 ACG Web 管理界面单击"系统管理"→"部署方式"命令,检查当前配置是否启用了"旁路部署"功能,如图 6-40 所示。当状态显示为红色时,表示该端口当前未启用旁路部署模式;反之,当状态显示为绿色时,表示该端口已经启用旁路部署模式。

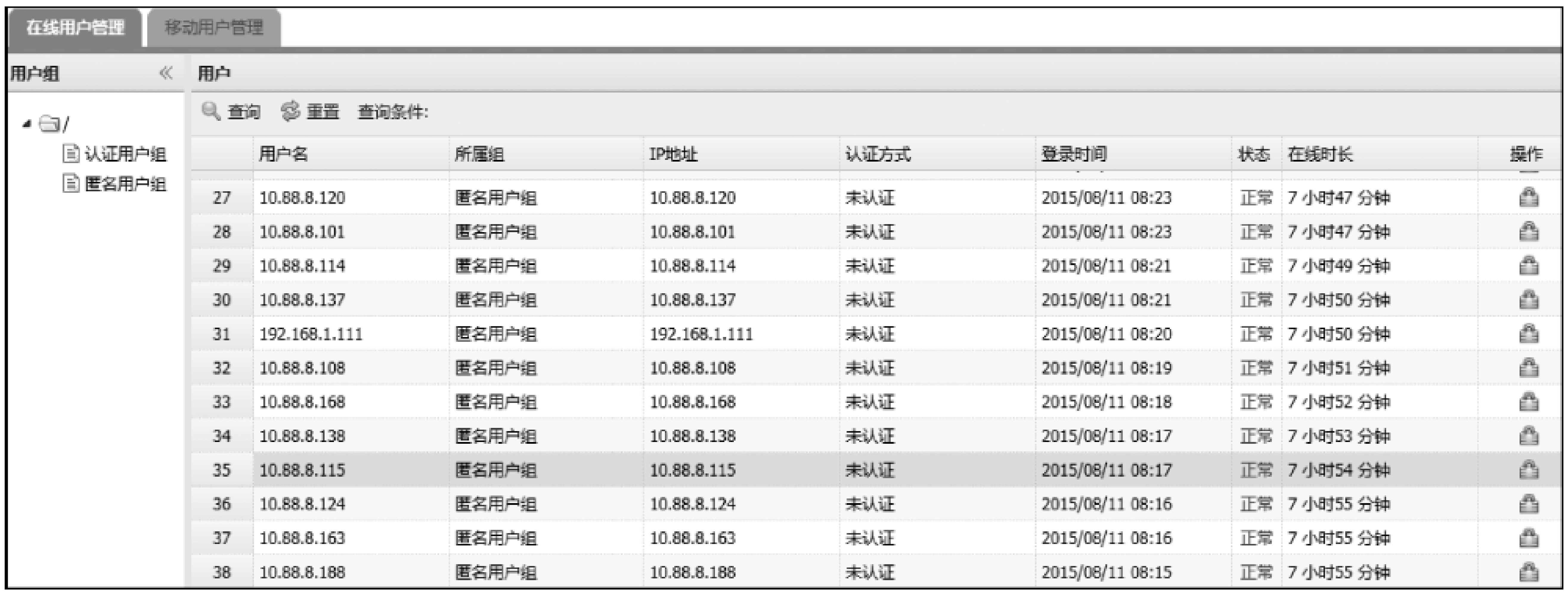


图 6-39　在线用户管理

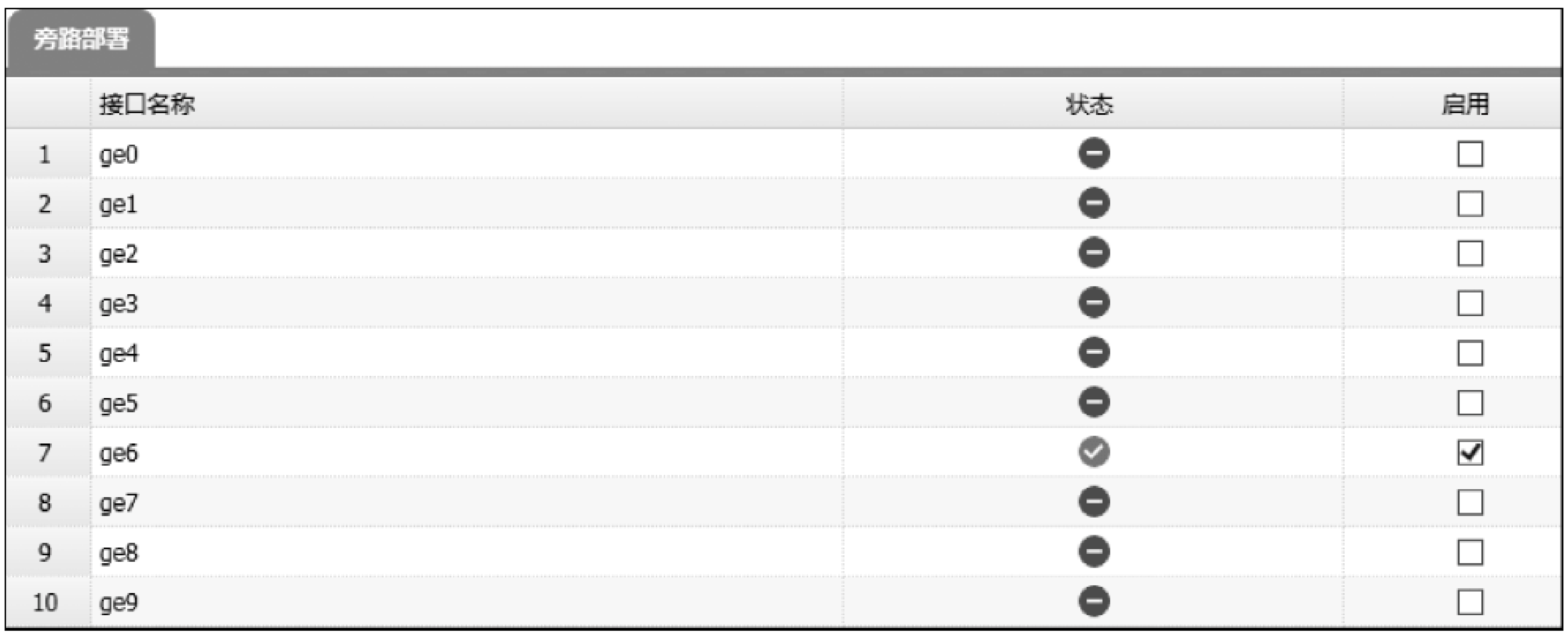


图 6-40　旁路部署

(5) 是否启用自定义 URL 过滤

ACG 设备支持自定义 URL 过滤和预定义分类 URL 过滤功能。若当前设备启用了自定义 URL 过滤，则需要先检查自定义 URL 配置是否正常，否则，可直接进行策略配置检查。

(6) 检查自定义 URL 配置

ACG 设备支持自定义 URL 过滤功能，可以由客户自行配置网站域名关键字进行审计过滤配置。在问题排查过程中需要注意检查自定义 URL 配置是否准确。

命令：无

例如：在 ACG Web 管理界面单击“对象管理”→“URL”→“自定义 URL”命令，如图 6-41 所示，检查各自定义 URL 配置是否启用准确。特别要注意检查“URL”字段是否正确。



图 6-41　自定义 URL

(7) 检查策略配置

ACG 设备 URL 过滤功能是通过策略配置实现的，因此必须重点检查策略配置是否正确。

URL 分类是根据 URL 请求将网站访问分成相应的类别。URL 分类库是进行分类的依据，已经内置在版本当中。用户也可以依据自己的需要，自行定义新的 URL 分类。通过网站策略对其进行引用，并启用该策略，可以对相关的用户起到网站控制的作用。这样可以通过 HTTP 协议为用户提供应用级的安全防护和访问限制。自定义 URL 分类若与预定义 URL 分类冲突，自定义 URL 的优先级更高。

若系统中同时配置了多条策略，要注意多条策略间的匹配顺序。若策略匹配条件中引用了地址对象、时间表等，还应注意其引用的对象配置是否正确。

命令：无

例如：在 ACG Web 管理界面单击“上网行为管理”→“策略配置”命令，选中相应的 IPv4 或 IPv6 策略，展开策略配置界面，检查 URL 审计配置是否正确。以图 6-42 为例，动作配置为“拒绝”，表示设备将组织最终用户访问以“H3C”为名称的自定义 URL。



图 6-42　URL 审计

（8）检查地址对象配置

当 ACG 配置 URL 过滤策略时，引用了地址对象，则需检查该策略引用的地址对象本身是否配置正确，避免造成地址匹配错误。

命令：无

例如：在 ACG Web 管理界面单击“对象管理”→“地址”命令，如图 6-43 所示，检查地址对象、地址组对象配置是否准确。特别要注意检查“名称”“内容”“排除地址”字段是否配置正确，检查地址组对象与地址对象的嵌套引用关系是否正确。



图 6-43　IPv4 地址对象

（9）检查时间表配置

当 ACG 配置 URL 过滤策略时，引用了时间表对象，则需检查该策略引用的时间表对象本身是否配置正确，避免造成地址匹配错误。同时还应注意检查设备当前时间是否正常，若设备系统时间错误，可通过手工重新指定或 NTP 服务进行同步。

命令：无

例如：在 ACG Web 管理界面单击“对象管理”→“时间表”命令，如图 6-44 所示，检查各时间表对象配置是否合理。特别要注意检查“名称”、时间计划字段是否配置正确。



图 6-44　时间表

(10) 检查访问网站日志

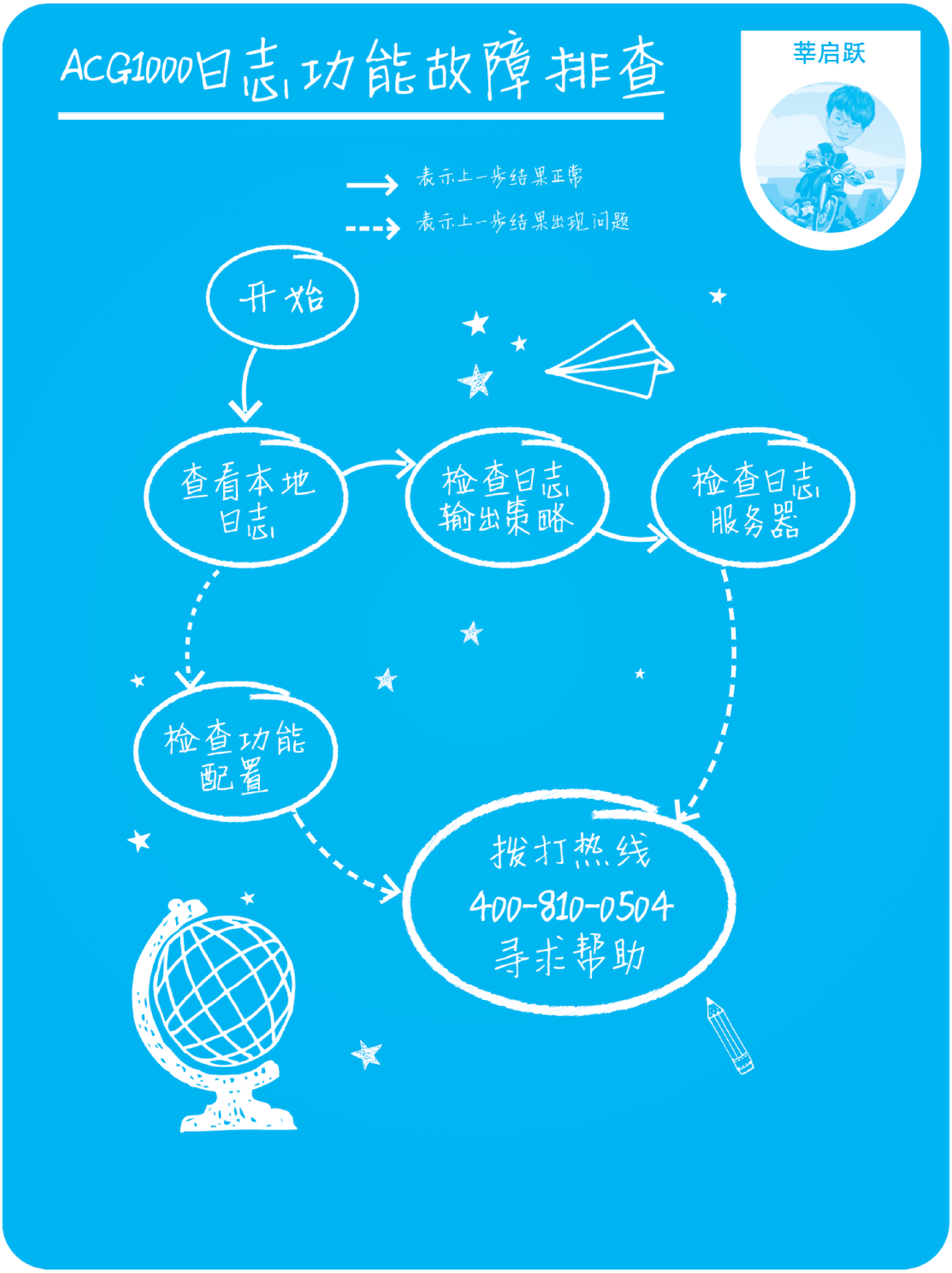
ACG 设备支持 URL 过滤日志审计功能，可以通过日志信息了解设备执行 URL 过滤策略的情况。在问题排查过程中，建议利用日志信息，分析判断管理员配置及设备工作是否正常。

命令：无

例如：在 ACG Web 管理界面单击"日志查询"→"网站访问日志"→"访问网站日志"命令，如图 6-45 所示，检查 URL 过滤日志信息，注意核对"用户""URL 分类"(包含自定义 URL)、"处理动作"等关键信息是否符合预期。



图 6-45　访问网站日志


ACG1000日志功能故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
查看本地日志
检查日志输出策略
检查日志服务器
检查功能配置
拨打热线
400-810-0504
寻求帮助

06 安全产品 > 6.1 安全协议 > 6.1.10 ACG1000 日志功能故障排查 > 步骤详解

1. 开始

ACG1000 是新款应用审计网关，提供全面充分的网络审计功能。日志功能至关重要，如果日志功能出现问题，审计功能得不到呈现。

ACG1000 日志功能故障排查的思路是：首先判断功能配置是否正确，再看日志输出策略和接收端是否存在问题。

2. 流程图相关操作说明

（1）查看本地日志

通过查看本地日志，判断本地日志生成是否正常。如果没有日志，则说明在功能配置上出现问题或者没有双向流量匹配。

例如：通过“日志查询→应用审计日志→搜索引擎日志”路径查看日志，如图 6-46 所示。



图 6-46　搜索引擎日志

发现存在搜索引擎日志则无问题。

如果没有日志，如图 6-47 所示，则需要检查一下配置了。



图 6-47　无搜索结果

（2）检查功能配置

每个审计项开启时都需要选择记录日志，否则日志无法输出。

例如：通过“上网行为管理→策略配置→IPv4 策略”路径查看，如图 6-48 所示，发现搜索引擎审计没有开启记录日志功能，其他审计类开启了。

此时需要单击修改成“记录日志”。

此外，还存在流量匹配不到审计策略导致没有日志产生的问题，如图 6-49 所示。双向流量是否匹配除了检查接口流量统计、检查匹配的条件设置是否正确之外，还可以开启全部审计，并记录日志，来判断是否能记录到某个流量的任何一种日志信息。如果某些日志无法显示，配置也正常，还可能是特征库不识别导致。



图 6-48 开启了其他审计类



图 6-49 IPv4 策略

（3）检查日志输出策略

确认本地日志产生后，有用户无法看到日志服务器侧日志。此时需要确定日志输出策略是否正确。

单击“系统管理”→“日志设定”命令，如图 6-50 所示，检查日志服务器设置情况。



图 6-50 日志服务器

然后再看"日志过滤"。需要单击"高级配置"选项查看详细功能。

说明：本地日志要记录，server 日志也要发送，不能选择不发送，如图 6-51 所示。默认情况下，日志过滤策略都是默认记录和发送的，不会有问题。

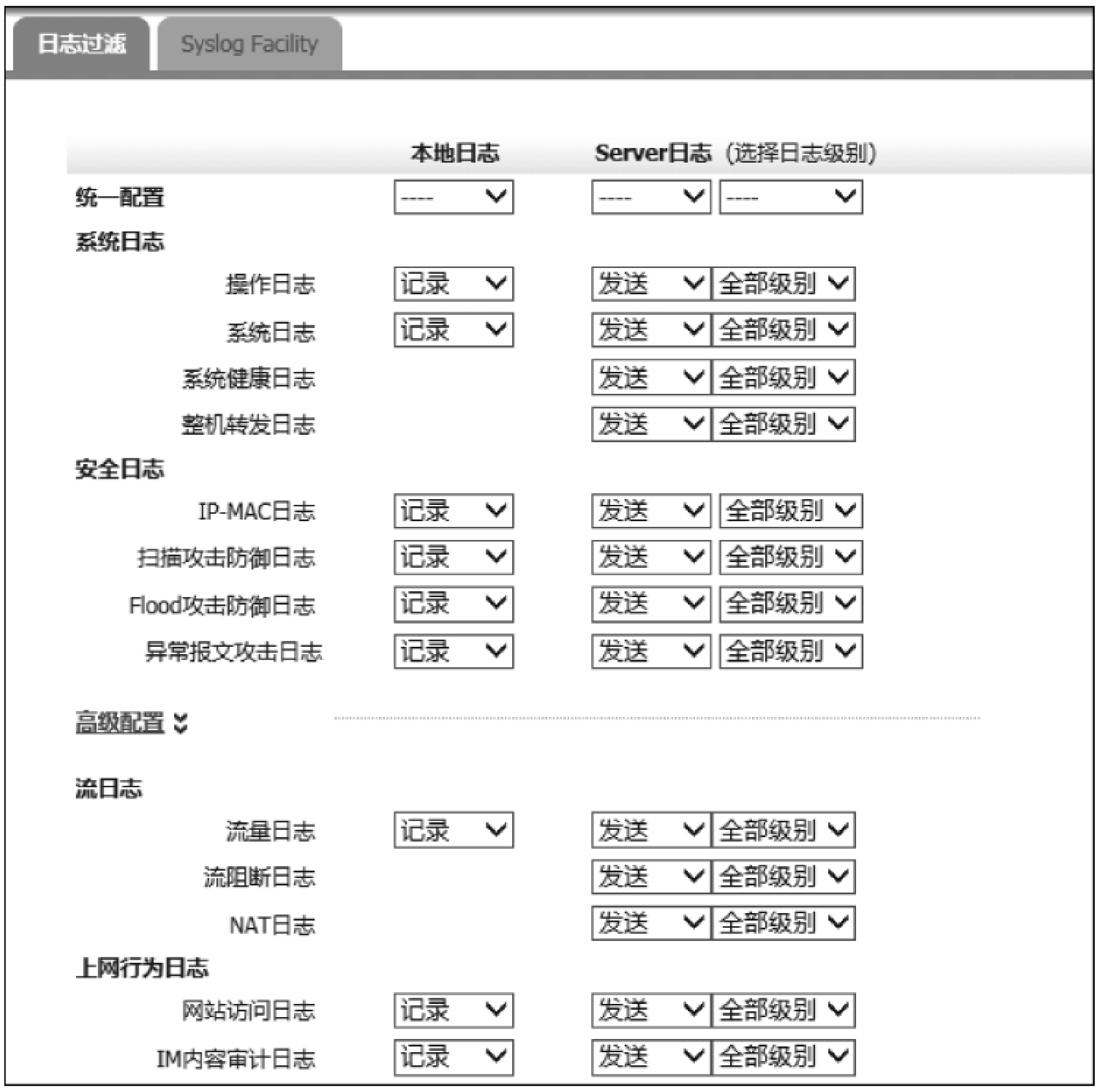


图 6-51　日志过滤

（4）检查日志服务器

检查设备日志功能配置后，来判断日志服务器侧能否收到日志报文。

可以在日志服务器上抓包来判断是否能收到目的端口是设定的日志输出端口的报文。如果没有收到，需要检查设备到服务器间网络是否连通。

如果有报文，但是服务器依旧不显示日志，可能存在以下情况。

① 服务器安装了防火墙等安全软件使报文丢弃。

② 日志管理软件的 License 没有授权管理功能。

③ 日志管理软件的后台数据库损坏。

①和②情况可以自行检查，③类情况则需要联系呼叫中心来远程恢复数据库。



防火墙CPU利用率高故障排查
表示上一步结果正常
表示上一步结果出现问题
西海华
开始
查看CPU利用率
查看CPU进程
收集进程详细信息
查看多核引擎利用率
查看会话统计
查看接口流量
查看异常流量并进行控制
拨打热线 400-810-0504寻求帮助

1. 开始

防火墙很多报文都要上送 CPU 处理，因此 CPU 利用率高是防火墙比较常见的问题，具体包括控制核利用率高和转发核利用率高。防火墙 CPU 利用率高问题定位故障的思路是：首先查看是 CPU 控制核利用率，找出占用 CPU 高的进程，根据进程进行相关处理；其次查看数据转发平面 CPU 利用率，如果转发平面 CPU 利用率比较高是因为数量流量太大，要注意查看网络中是否存在环路或者攻击等异常流量。

2. 流程图相关操作说明

(1) 查看 CPU 利用率

直接通过命令查看防火墙 CPU 利用率，体现的是防火墙控制核的利用率情况，正常情况下，防火墙控制平面 CPU 的利用率应该小于 20%。

命令：*display cpu-usage*

例如：通过命令查看防火墙 CPU 占用率。

```
[H3C]display cpu-usage
Unit CPU usage:
        2% in last 5 seconds
        1% in last 1 minute
        1% in last 5 minutes
```

(2) 查看 CPU 进程

控制平面 CPU 负责各种协议报文的处理，通过查看 CPU 任务进程，可以了解每个进程占用的 CPU 资源情况。

命令：*_hidecmd*

display cpu-usage task

例如：通过命令查看进程。

```
[H3C]_hidecmd
[H3C-hidecmd]display cpu-usage task
-------- Current CPU usage info --------
CPU Usage Stat. Cycle: 2 (Second)
CPU Usage              : 9%
CPU Usage Stat. Time : 2013-12-25   10:02:18
CPU Usage Stat. Tick : 0x587(CPU Tick High) 0x6ab6e0(CPU Tick Low)
Actual Stat. Cycle    : 0x0(CPU Tick High) 0x8dcc3df(CPU Tick Low)

TaskName          CPU          Runtime(CPU Tick High/CPU Tick Low)
  VIDL            91%                  0/  81913c8
  TICK             0%                  0/     64ed4
 STMR              1%                  0/   1b0e93
 DRVT              0%                  0/     50d5f
 TMSG              0%                  0/     3584f
  IPCB             0%                  0/       ee49
 RPCQ              0%                  0/     29954
```

```
     ADJ6          0%            0/     122a
     IPCM          0%            0/      ae3
      OMS          0%            0/      eb8
      DEV          0%            0/     2529
     SOCK          0%            0/     139b
     ADJ4          0%            0/     38a2
     LAGG          0%            0/      a6a
     MSTP          0%            0/      bc6
      ARP          0%            0/     faf3
       IP          0%            0/    2d301
     FSLH          0%            0/      790
     FSLR          0%            0/     5f6c
     NTPT          0%            0/      d74
     VTYD          0%            0/     bfb2
     DHCP          0%            0/     6f37
       ND          0%            0/     a37c
      ACM          0%            0/    1c426
       LS          0%            0/     5cda
     RDSO          0%            0/     578d
       SC          0%            0/     16ab
      IKE          0%            0/    2db49
     L2TP          0%            0/     575c
     ULOG          0%            0/     6fdd
     STND          0%            0/     2091
     ROUT          0%            0/    49773
     IFNT          0%            0/      b21
     IPFF          0%            0/      87f
     TNLT          0%            0/      988
      vt1          5%            0/   84965b
```

进程任务说明。

```
TaskName        CPU        Runtime(CPU Tick High/CPU Tick Low)
    VP           0%          0/       430
  VIDL          56%          0/  71fc04a2              //空闲资源
  TICK           0%          0/    abf304
  STMR           1%          0/   3446bab              //定时器进程
  DRVT           0%          0/    b492b7
  TMSG           0%          0/    17bd5f5             //核间消息同步
  IPCB          22%          0/  2dfed35a              //信息通道
  RPCQ           0%          0/    3d0999
  ADJ6           0%          0/      8b1e              //IPV6 邻接表
  IPCM           0%          0/     112d3
  INFO           0%          0/   13c201a              //信息中心
   OMS           0%          0/     24c52
   DEV           0%          0/     31c44
  SOCK           0%          0/    1574c6              //本地 socket
  ADJ4           0%          0/     1f7af              //IPV4 邻接表
   ACL           0%          0/     71db6              //ACL
  LAGG           0%          0/     14482              //链路聚合
  MSTP           0%          0/     15aab              //MSTP 进程
```

```
ARP        0%     0/  244ff4     //ARP 进程
IP         0%     0/  443d6d
FSLH       0%     0/    eff7
FSLR       0%     0/   a1168     //SSL VPN 进程
NTPT       0%     0/   1bdcb     //NTP 时钟同步
VTYD       0%     0/   970a7
ND         0%     0/   f86e9     //邻居表
AGNT       0%     0/   ac265
ACM        0%     0/  317f07
LS         0%     0/   81186
RDSO       1%     0/ 3a1eadd
IKE       14%     0/1d50a365     //IKE 进程
L2TP       0%     0/   a64d0     //L2TP VPN
ULOG       0%     0/   a841c     //会话日志
MFIB       0%     0/    51c8     //应该是 FIB 表
STND       0%     0/   3b13c
ROUT       0%     0/  6c4f0e     //路由
IFNT       0%     0/   15dc7     //应该是接口相关
IPFF       0%     0/   27b87     //快转
DNS        0%     0/   92a5a     //DNS
co0        0%     0/  8c2cb8     //串口
IPSP       0%     0/    e74e     //—IPSEC VPN
DHBK       0%     0/    eae2     //双机热备
HDQ0       0%     0/    918a     //Web 访问
```

比如 INFO 进程很高，可以看看设备日志开启情况，是否开启了大量日志，可以关闭一些日志，观察是否有改善。

(3) 收集进程详细信息

如果现场无法根据上面的进程信息解决问题，可以进一步收集详细反馈到技术支持中心。V5 防火墙控制核 CPU 进程信息收集方法如下，以 INFO 为例。

① 查看 CPU 各任务利用率，找到利用率高的任务。

```
[H3C]_hidecmd
[H3C-hidecmd]display cpu-usage task
-------- Current CPU usage info --------
CPU Usage Stat. Cycle: 26 (Second)
CPU Usage              :82%
CPU Usage Stat. Time : 2013-12-30   10:05:31
CPU Usage Stat. Tick : 0x1fbb(CPU Tick High) 0x86aa1ed0(CPU Tick Low
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x67f8409a(CPU Tick Low)

 TaskName      CPU          Runtime(CPU Tick High/CPU Tick Low)
   VIDL         5%                0/641b12b2
   TICK         0%                0/  45b991
   STMR         1%                0/  162f980
   DRVT         0%                0/  352ba2
   TMSG         0%                0/  2786c2
   IPCB         0%                0/   a6258
   RPCQ         0%                0/  1d9343
```

```
       ADJ6          0%              0/      3a5f
       IPCM          0%              0/      7a16
       INFO         61%              0/     25334
        OMS          0%              0/      c404
        DEV          0%              0/     27280
       SOCK          0%              0/     11524
       ADJ4          0%              0/      f24a
        ACL          0%              0/     20de3
       LAGG          0%              0/      86c3
       MSTP          0%              0/      9929
        ARP          0%              0/     c57ae
         IP          0%              0/    2243ae
       IFNT          0%              0/      985b
       IPFF          0%              0/      7d31
       TNLT          0%              0/      b096
        vt0          0%              0/   vd8e7e6
```

② 进一步根据任务名称查找其 ID。

```
[H3C]_hidecmd
[AC-hidecmd]display task
name          Tid   Vid  TSize  Mod  priority     Status        Total/Max/Last(Millsecs)
-------------------------------------------------------------------------------------
 VMON  8033ec00   1    40    N    100     eventblock          0/     0/      0
   VP  837b9000   2    40    N    140     eventblock        114/     0/      0
 VIDL  8033ea00   3    40    P      1   preemptready  516602008/     9/      5
 TICK  8033e800   4    40    P    250   preemptready    1414607/     0/      0
 STMR  8033e600   5    40    N    150     eventblock    7284583/    27/      0
 DFWD  8033e400   6    40    N    100     eventblock          0/     0/      0
 DRVT  8033e200   7    40    N    100     eventblock    1090117/    86/      0
 TMSG  8033e000   8    40    N    100     eventblock     678471/     1/      0
 IPCB  83dc2e00   9    40    N    140     eventblock     221234/     0/      0
 IPCD  83dc2c00  10    40    N    100     eventblock          0/     0/      0
 RPCQ  83dc2a00  11    40    N    140     eventblock     613831/     0/      0
 RPCD  83dc2800  12    40    N    140     eventblock          0/     0/      0
  PAT  83dc2600  13    40    N    100     eventblock          3/     0/      0
 MACF  83dc2400  14    40    N    100     eventblock          3/     0/      0
 ADJ6  83dc2200  15    40    N    100     eventblock       4461/     0/      0
 IPCM  83dc2000  16    40    N    100     eventblock       9560/     0/      0
  CFM  83dc3e00  17    40    N    100      queblock       3025/   563/    563
 INFO  83dc3c00  18    40    N    100   normalready       8042/     8/      0
 LGFT  83dc3a00  19    40    N    100     eventblock        163/     9/      0
  OMS  83dc3800  20    40    N    100     eventblock      15542/            0/
  DEV  83dc3600  21    40    N    140     eventblock      48100/     0/      0
 WORK  83dc3400  22    40    N    100     eventblock          0/     0/      0
```

③ 在按照 ID 把这个进程的当前堆栈信息打印出来。

```
[H3C]_hidecmd
[H3C-hidecmd]display task 18
```

```
Task name                    : INFO
Task PLAT Index              : 18
Task OS Index                : 0x83dc3c00
Task StackTop                : 0x80330000
Task priority                : 100
Task Status                  : normalready
Last run time(CPU Tick)      : 0x0(high)   0x8357(low)
Max run time(CPU Tick)       : 0x0(high)   0x87dd3(low)
Total run time(CPU Tick)     : 0x0(high)   0x20437657(low)
Stack Information:
  0x8022d780
  0x802313dc
  0x80231ba8
  0x813ef48c
  0x813dc6a0
  0x813dc234
  0x813dbf7c
  0x81607940
```

将收集的上述信息，连同诊断信息和配置文件一起反馈给技术支持中心。

(4) 查看多核引擎利用率

多核引擎利用率就是数据平面 CPU 的利用率，通过查看防火墙多核引擎利用率，可以了解防火墙流量在多核上的转发是否负载均匀，是否存在异常流量等信息。默认情况下防火墙多核之间是逐包转发，各数据核利用率应该基本一致才对，另外可以通过命令将防火墙改成逐流转发，这样各个核心可能存在一些差距。

命令：*_hidecmd*

tshow mainboard cpu-usage all

例如：通过命令查看防火墙转发核占用率，发现其中一个核的利用率明显偏高(核 1～3 不负责业务数据的转发，所以利用率显示为 0)。说明有异常流量分发到这个核上，可能会导致该数据核挂死，可以通过会话或者抓包的方式找到对应的流量。

```
[H3C]_hidecmd
[H3C-hidecmd]tshow mainboard cpu-usage all
  VCPU usage information:
    1     0%
    2     0%
    3     0%
    4     5%
    5     5%
    6     5%
    7     5%
    8     5%
    9     5%
    10    5%
    11    5%
    12    98%
    13    5%
    14    5%
    15    5%
    16    5%
```

```
    17    5%
    18    5%
    …
```

(5) 查看会话统计

如果防火墙的流量太大或者防火墙收到攻击流量,会话统计信息里面的会话总数、半开连接数、会话新建速率等参数会增加很多,可以通过查看会话明细或者抓包的方法确认异常流量。

命令: *display session statistics*

例如: 通过命令查看会话统计信息。

```
[H3C]display session statistics
Current session(s):2959981
          Current       TCP session(s): 2827396
                   Half-Open: 2765555        Half-Close: 24194
          Current       UDP session(s): 132052
          Current      ICMP session(s): 532
          Current    RAWIP session(s): 1

Current relation table(s): 14

Session establishment rate:       60815/s
          TCP       Session establishment rate:        59599/s
          UDP       Session establishment rate:         1207/s
…
```

查看会话表中的 Half-open 和 Half-close,可以判断网络中是否有 flood 攻击流量。

查看新建会话速率 Session establishment rate,可以判断网络中是否有大量异常新建会话流量,是否超过设备规格。

查看关联表 Current relation table(s),可以确定网络中是否有大量不走快转的流量。

(6) 查看接口流量

如果防火墙的会话统计信息偏高,还可以进一步查看防火墙接口流量,确定经过防火墙的出入流量速率分别是多大,是否超过设备处理能力。

命令: *reset counters interface interface-type interface-number*

display interfacei interface-type interface-number

例如: 通过命令查看接口流量。

```
<H3C>reset counters interface GigabitEthernet 0/0
[H3C]display interface GigabitEthernet 0/0
GigabitEthernet0/0 current state: Up
Line protocol current state: Up
Description: GigabitEthernet0/0 Interface
The Maximum Transmit Unit is 1500
Internet Address is 10.153.42.83/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e27b-f27b
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e27b-f27b
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s, Full-duplex, link type is autonegotiation
```

```
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queuing : Size/Length/Discards)   0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)   0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)   0/75/0
Last clearing of counters: Never
    Peak value of input: 7239195 bytes/sec, at 2013-12-1 11:26:3
    Peak value of output: 92335 bytes/sec, at 2013-12-2 3:22:18
    Last 300 seconds input rate 324 bytes/sec, 2592 bits/sec, 4 packets/sec
    Last 300 seconds output rate 71 bytes/sec, 568 bits/sec, 1 packets/sec
    Input: 126033021 packets, 0 jumboes, 53336845783 bytes, 126033021 buffers
           6284150 broadcasts, 119098432 multicasts, 0 pauses
           0 errors, 0 runts, 0 giants
           0 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
    Output:587606 packets, 101386403 bytes, 587606 buffers
           376 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 underruns, 0 collisions
           0 deferred, 0 drops, 0 lost carriers
```

(7）查看异常流量并进行控制

如果防火墙的某一个数据核的利用率偏高，但是会话统计信息正常，说明是某一条数据流流量太大，这个数据流很可能是环路或者攻击，可以通过抓包或者查看会话明细的方法找到异常流量。防火墙的会话记录了每一条数据流的详细信息，根据会话可以看到数据流的 IP 地址、端口、协议、会话状态，收发报文数等信息。找到异常流量后可以通过连接数限制、防攻击、黑名单或者在其他上下行设备上配置访问控制列表等方法进行控制。

命令：*display session table verbose*

例如：通过命令可以看到其中一条数据流收发报文数很大，明细存在异常。

```
[H3C]display session table verbose
Initiator:
  Source IP/Port : 10.153.42.16/2077
  Dest IP/Port   : 10.153.42.59/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 10.153.42.59/80
  Dest IP/Port   : 10.153.42.16/2077
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP       State: TCP-EST
Start time: 2013-12-25 10:55:04   TTL: 6s
Root                         Zone(in):Untust
                             Zone(out):Trust
Received packet(s)(Init): 3564281 packet(s) 712856200 byte(s)
Received packet(s)(Reply):3258462 packet(s) 645175476 byte(s)
```


防火墙NAT故障排查
表示上一步结果正常
表示上一步结果出现问题
西海华
开始
查看会话
检查NAT配置
检查域间策略
排查异常侧网络连通性
检查路由
拨打热线
400-810-0504寻求帮助

1. 开始

NAT 是防火墙最主要的功能之一，防火墙的会话记录了 NAT 转化的所有信息，排查 NAT 的问题时要结合会话查看。防火墙 NAT 问题定位故障的思路是：先查看防火墙上是否有会话，如果没有会话先判断防火墙是否收到报文，然后依次检查防火墙 NAT、域间策略和路由等相关配置，确认报文转发路径正确且没有被过滤；如果防火墙上有会话，就检查 NAT 前后的地址是否正确，收发报文是否正常，如果收发报文不正常需要根据会话报文统计情况进一步排查内外网路由。

2. 流程图相关操作说明

（1）查看会话

要想确认设备是否进行了正常的 NAT 转换，最直接的方法就是查看设备的会话信息，根据会话可以看到 NAT 转换前后的地址和对应关系。

命令：*display session table source-ip x.x.x.x destination-ip x.x.x.x verbose*

例如：通过命令可以看到源为 192.168.5.1 的数据报文经过防火墙 NAT 转化后地址变成了 60.191.66.139，报文收发也正常。

```
<H3C>display session table source-ip 192.168.5.1 destination-ip 60.170.255.12 verbose
Initiator:
  Source IP/Port : 192.168.5.1/2048
  Dest IP/Port   : 60.170.255.12/3
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port :60.170.255.12/0
  Dest IP/Port   : 60.191.99.139/1026
  VPN-Instance/VLAN ID/VLL ID:
Pro: ICMP(1)      App: unknown          State: ICMP-CLOSED
Start time: 2013-12-24 11:06:56   TTL: 30s
Root                        Zone(in): Trust
                            Zone(out): Untrust
Received packet(s)(Init): 459 packet(s) 38556 byte(s)
Received packet(s)(Reply): 459 packet(s) 38556 byte(s)

Total find: 1
```

（2）排查异常侧网络连通性

如果根据会话查看防火墙地址转换正常，但是没有收到响应方的报文，需要仔细检查防火墙到报文源目的两端地址的路由，同时也需要仔细检查内部网络或者服务器到防火墙的路由，确保数据流的来回报文都经过防火墙。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看内网和外网的路由都正常。

```
<H3C>display ip routing-table 60.170.255.12
Routing Table : Public
```

```
Summary Count : 1

Destination/Mask   Proto   Pre   Cost      NextHop          Interface

0.0.0.0/0          Static  60    0         60.191.99.1      Vlan11
<H3C>display ip routing-table 192.168.5.1
Routing Table : Public
Summary Count : 2

Destination/Mask   Proto   Pre   Cost      NextHop          Interface

0.0.0.0/0          Static  60    0         60.191.99.1      Vlan11
192.168.5.0/24     Static  60    0         10.0.0.2         Vlan10
```

(3) 检查 NAT 配置

如果防火墙会话不正常,先查看 NAT 的配置是否正确,这里分以下几种情况。

① 检查 nat outbound 配置。

命令:*display nat address-group x*

display nat bound

display acl x

例如:通过命令查看 NAT 的地址池、ACL 规则以及下发接口是否正常,ACL 规则、ACL 的匹配次数等相关配置。

```
<H3C>display nat address-group 1
NAT address-group information:
  1       : from 60.191.99.139       to 60.191.99.139

<H3C>display nat bound
NAT bound information:
  There are currently1 nat bound rule(s)
  Interface:Vlan-interface11
  Direction: outbound ACL: 3000 Address-group: 1 NO-PAT: N Port-Preserved :N
    VPN-instance: ---

<H3C>display acl 3000
Advanced ACL   3000, named -none-, 2 rules,
ACL's step is 5
  rule 0 permit ip source 192.168.5.0 0.0.0.255 (3 times matched)
  rule 5 permit ip source 10.0.0.0 0.0.0.255
```

② 检查 NAT Server 配置。

命令:*display nat server*

```
[H3C]dis nat server
NAT server in private network information:
  There are currently 1 internal server(s)
  Interface: Vlan-interface11, Protocol: 6(tcp)
    Global:     60.191.99.20 : 8080
    Local :       192.168.5.1 :80
```

③ 检查 NAT Static 配置。

命令：*display nat static*

```
[H3C]display nat static
NAT static information:
  There are currently 1 NAT static configuration(s)
  single static:
    Local-IP        : 192.168.5.2
    Global-IP       : 60.191.99.21
    Local-VPN       : ---
    Global-VPN      : ---

NAT static enabled information:
  Interface                                   Direction
  Vlan-interface11                            out-static
```

④ 检查 NAT Outbound 配置。

防火墙双机热备组网情况下，要求两台防火墙地址池优先级不同，主防火墙优先级高，备防火墙优先级低。另外如果地址池地址和接口地址在同一网段时，NAT 后面需要 track vrrp，否则两台设备的地址池都会响应 ARP，防火墙上下行设备学习 ARP 的时候会出现异常，track vrrp 以后，只有 master 设备的地址池地址可以响应 ARP。

命令：*display current-configuration | begin nat address-group*

display current-configuration | include nat outbound

```
<H3C> display current-configuration | begin nat address-group
nat address-group 1 60.191.99.139 60.191.99.139 level 1
<H3C>display current-configuration | include nat outbound
nat outbound 3000 address-group 1 track vrrp 11
备防火墙:
<H3C> display current-configuration | begin nat address-group
nat address-group 1 60.191.99.139 60.191.99.139 level 0
<H3C>dis current-configuration | include nat outbound
nat outbound 3000 address-group 1 track vrrp 11
```

⑤ 检查 NAT Server 配置。

如果 NAT Server 的公网地址和接口地址在同一网段时也需要 track vrrp。

命令：*display current-configuration | include nat server*

```
主防火墙:
[H3C]display current-configuration | include nat server
nat server protocol tcp global 60.191.99.20 any inside 192.168.5.1 any track vrrp 11
备防火墙:
[H3C]display current-configuration | include nat server
nat server protocol tcp global 60.191.99.20 any inside 192.168.5.1 any track vrrp 11
```

⑥ 检查 NAT Static 配置。

同理，如果 NAT Static 的公网地址和接口地址在同一网段时也需要 track vrrp。

命令：*display current-configuration | include nat outbound static*

```
[H3C]display current-configuration | include nat outbound static
nat outbound static track vrrp 11
备防火墙:
[H3C]display current-configuration | include nat server
nat outbound static track vrrp 11
```

(4) 检查域间策略

防火墙所有报文转发都是基于安全区域的,所有除了检查 NAT 配置外还需要检查安全区域及域间策略的配置,确保 NAT 的数据流不会被防火墙丢弃。

首先查看防火墙设备上相关业务接口是否已经正确地加入安全域。

命令:*display current-configuration | begin zone*

例如:通过命令查看,可以确认内外两个业务接口已经正确加入安全域。

```
<H3C>dis current-configuration | begin zone
zone name Management id 0
 priority 100
 import interface GigabitEthernet0/1
zone name Local id 1
 priority 100
zone name Trust id 2
 priority 85
 import interface Vlan-interface10
zone name DMZ id 3
 priority 50
zone name Untrust id 4
 priority 5
 import interface Vlan-interface11
```

确认接口已经加入安全域后,查看相关域间策略,确认不同优先级间的状态是允许状态,或者保证发起方为高优先级方,保证数据流的正常建立。对于从外网主动发起访问的连接,比如 NAT Server 和 NAT Static,需要配置域间策略允许报文通过,这里要重点注意:防火墙接口数据报文的处理流程是先处理 NAT 再处理报文过滤,所以对于 NAT Server 和 NAT Static,域间策略允许的目的地址是私网地址。

命令:*display current-configuration | begin interzone*

例如:通过命令查看,可以确认 untrust 到 trust 的域间策略已经部分放通。

```
[H3C]display current-configuration | begin interzone
 interzone source Untrust destination Trust
  rule 0 permit
   source-ip any_address
   destination-ip 192.168.5.1/0.0.0.0
   service any_service
   rule enable
```

(5) 检查路由

如果防火墙 NAT 和域间策略配置都正确,但是会话不正常,可以检查下路由信息。如果完全没有会话信息,可能是设备没有收到数据报文,如果 NAT 地址转换错误,可能是报文走了不同的出接口。

命令:*display ip routing-table x.x.x.x*

例如：通过命令查看防火墙路由相关是否正确。

```
<H3C>display ip routing-table 60.170.255.12
Routing Table : Public
Summary Count : 1

Destination/Mask   Proto   Pre   Cost   NextHop        Interface

0.0.0.0/0          Static  60    0      60.191.99.1    Vlan11
<H3C>display ip routing-table 192.168.5.1
Routing Table : Public
Summary Count : 2

Destination/Mask   Proto   Pre   Cost   NextHop        Interface

0.0.0.0/0          Static  60    0      60.191.99.1    Vlan11
192.168.5.0/24     Static  60    0      10.0.0.2       Vlan10
```


防火墙Web网管故障排查
表示上一步结果正常
表示上一步结果出现问题
沈博文
开始
查看设备连通性
是否使用HTTPS方式
检查HTTPS配置
检查设备本地端口连接状态
检查管理口配置
检查HTTP配置
检查Web用户配置
检查浏览器设置
拨打热线
400-810-0504寻求帮助

1. 开始

Web 管理是 V5 防火墙最主要的管理方式之一，Web 网管需要配合浏览器来使用，所以问题的排查不能仅仅针对防火墙设备，还需要从网页浏览器入手。Web 网管定位故障的思路是：首先检查客户端和防火墙管理口之间的连通性；其次查看防火墙 Web 网管相关配置是否正确、本地端口监听是否正常；再次检查 Web 登录的用户是否合法，防火墙在线用户数以及连接数是否在设备允许的范围内；最后检查浏览器的版本、设置等是否正确。

2. 流程图相关操作说明

(1) 查看设备连通性

通过 Web 方式管理防火墙，首先要确保客户端到管理口能够正常通信，可以使用 ping 等手段简单测试，或者通过命令行登录防火墙查看是否建立了相关会话。如果通信不正常，需要先检查下防火墙的配置是否正确，然后再检查管理流量所经过的网络通信是否正常，是否存在报文被中间设备过滤的情况。

命令：*ping x.x.x.x*

display session table source-ip x.x.x.x verbose

```
[H3C]ping 192.16.0.1
  PING 1.1.1.1: 56   data bytes, press CTRL_C to break
    Reply from 1.1.1.1: bytes=56 Sequence=0 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 1.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 1.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

[H3C]display session table source-ip 192.168.0.2 verbose
Initiator:
  Source IP/Port :192.168.0.2/17456
  Dest IP/Port   :192.168.0.1/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port :192.168.0.1/80
  Dest IP/Port   :192.168.0.2/17456
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP                State: TCP-EST
Start time: 2000-05-02 15:33:16   TTL: 3591s
Root                          Zone(in): Management
                              Zone(out): Local
Received packet(s)(Init): 2 packet(s) 92 byte(s)
Received packet(s)(Reply): 1 packet(s) 44 byte(s)
```

(2) 检查管理口配置

如果连通性测试不通过，请检查接口地址和接口状态是否正常，如果接口地址和接口状态正常，再检查接口是否加入安全区域，通常情况下最好把管理口加入管理区域。

命令：*display ip interface interface-type interface-number*

zone add interface interface-type interface-number to management

```
[H3C]display ip interface GigabitEthernet 0/1
GigabitEthernet2/1 current state :Up
Line protocol current state :Up
Internet Address is 192.168.0.1/24 Primary

[H3C]_h
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]zone add interface GigabitEthernet 0/1 to management
```

(3) 检查 HTTPS 配置

如果防火墙启用了 HTTPS 的管理方式,确认防火墙 HTTPS 服务是否开启,配置是否正确,以及是否通过访问控制列表限制了用户访问等。

命令:*display ip https*

display acl xxxx

例如:通过命令查看到当前使用 HTTPS 的管理方式,HTTPS 的登录端口号是 443,关联了 acl 2000,状态为激活状态。

```
<H3C>display ip https
HTTPS port: 443
SSL server policy:
Certificate access-control-policy:
Basic ACL: 2000
Current connection: 0
Operation status: Running

<H3C>display acl 2000
Basic ACL  2000, named -none-, 1 rules,
ACL's step is 5
  rule 0 permit source 10.165.136.202 0 (122 times matched)
```

如果 HTTPS 管理方式启用了设备默认配置,没有将 SSL 服务器端策略与 HTTPS 服务进行关联,此时 HTTPS 使用设备默认的自签名证书,可通过命令检查默认证书是否存在。

命令:*display pki certificate ca domain default*

display pki certificate local domain default

例如:通过命令查看默认 CA 证书,通常其 CN 为"cademo",有效期 10 年。

```
<H3C>display pki certificate ca domain default
Certificate:
    Data:
        ...
        Issuer:
            CN=cademo
        Validity
            Not Before: Nov  9 01:48:34 2007 GMT
            Not After : Nov  9 01:48:34 2017 GMT
        Subject:
            CN=cademo
...
```

例如：通过命令查看默认 Local 证书，通常其 CN 为“cademo”，有效期 10 年。

```
<H3C>display pki certificate local domain default
Certificate:
    Data:
        …
        Issuer:
            CN=cademo
        Validity
            Not Before: Nov 12 07:34:55 2007 GMT
            Not After : Nov  9 01:48:34 2017 GMT
        Subject:
            C=CN
            ST=localdemo
            L=localdemo
            O=localdemo
            OU=localdemo
            CN=localdemo
        …
```

如果将 SSL 服务器端策略与 HTTPS 服务进行了关联，还请检查设备 PKI 配置是否正确（请参考云图“PKI 故障排查”）。

（4）检查 HTTP 配置

如果防火墙启用了 HTTP 的管理方式，确认防火墙 HTTP 服务是否开启，使用的端口号以及是否通过访问控制列别限制了用户访问。

命令：*display ip http*

display acl xxxx

例如：通过命令查看到当前使用了 HTTP 的管理方式，HTTP 的登录端口号是 80，状态为激活状态，关联了 acl 2000。

```
<H3C>display ip http
HTTP port: 80
Basic ACL: 2000
Current connection: 0
Operation status: Running

<H3C>display acl 2000
Basic ACL  2000, named -none-,1 rules,
ACL's step is 5
  rule 0 permit source 10.165.136.202 0 (122 times matched)
```

（5）检查 Web 用户配置

确认用户状态和用户登录界面配置正确，查看对应的用户状态是否为激活状态，是否赋予用户相关的登录方式和用户权限，开启了何种认证方式，并且确认当前在线的 Web 用户数量是否达到上限，目前防火墙 Web 同时登录的最大用户数是 5。

命令：*display local-user user-name user-name*

display user-interface vty vty-number

display web users

例如：通过命令查看，可以看到当前本地用户状态为 Active，授权给用户的登录方式为

telnet/web,用户的管理级别为3级；用户界面配置的认证方式为AAA认证,示例使用了本地用户认证,如果使用了radius服务器作为用户认证服务器需另外检查radius服务器状态；当前在线Web用户数量为1个。

```
<H3C>display local-user user-name admin
The contents of local user admin:
 VD
 State:                    Active
 ServiceType:              telnet/web
 Access-limit:             Disabled          Current AccessNum: 0
 User-group:               system
 Bind attributes:
 Authorization attributes:
 User Privilege:           3
Total 1 local user(s) matched.
<H3C>display user-interface vty 0
  Idx   Type      Tx/Rx      Modem Privi Auth  Int
  49    VTY 0                -     0     A     -
<H3C>dis web users
UserID    Name    Language   Level         State    LinkCount LoginTime LastTime
abb30000  h3c     Chinese    Management Enable      0         08:52:22  08:52:30
```

（6）检查设备本地端口连接状态

确认防火墙本地监听端口是否正常,另外设备Web管理Established状态的本地连接数上限值为100,一旦超过上限新的连接就不能建立；如果出现超出上限的现象,建议通过配置ACL的方式限制登录的用户数。

命令：*display tcp status*

ip http acl xxxx

ip https acl xxxx

display acl xxxx

例如：通过命令查看,可以看到当前防火墙监听了本地端口80和443,而且Established状态连接数存在1条,并建立acl 2000,仅允许合法的网管地址管理防火墙。

```
[H3C]display tcp status
 * : TCP MD5 Connection
TCPCB      Local Add:port       Foreign Add:port     State
10f5cfc0   0.0.0.0:443          0.0.0.0:0            Listening
105e0c60   0.0.0.0:80           0.0.0.0:0            Listening
1103a820   10.255.255.23:80     10.255.255.1:17331   Established

[H3C]ip http acl 2000

[H3C]display acl 2000
Basic ACL  2000, named -none-, 1 rules,
ACL's step is 5
rule 0 permit source 10.165.136.202 0 (122 times matched)
```

（7）检查浏览器设置

防火墙Web网管支持的浏览器包括：Microsoft Internet Explorer 6.0 SP2及以上版本、Mozilla Firefox 3.0及以上版本、Google Chrome 2.0.174.0及以上版本,其中Microsoft

Internet Explorer 9.0 以上(包括)版本最好开启兼容模式。如果版本在上述范围之内,仍然无法登录防火墙 Web 界面,请检查浏览器是否开启代理,另外,如果是设备升级后出现界面显示错误或不全的问题,可以通过清空浏览器缓存解决。

例如:查看 IE 浏览器的版本,如图 6-52 所示。



图 6-52 查看 IE 浏览器版本

设备的软件版本变化后,在通过 Web 网管登录设备时,建议先清除浏览器的缓存数据,否则 Web 网管的内容可能无法正确显示。

例如:清除 IE 浏览器缓存,如图 6-53 所示。



图 6-53 清除 IE 浏览器缓存


防火墙丢包故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
煎 饼
开始
是否本防火墙丢包
检查设备端口状态统计
检查CPU/内存利用率
检查虚拟分片重组
检查会话统计
检查快速转发
排查其他设备问题
拨打热线
400-810-0504
寻求帮助

1. 开始

防火墙丢包问题定位故障的思路是：首先确定发生丢包的具体位置和丢弃报文方向，然后再具体分析产生丢包的原因。在现场条件允许的前提下，最好先利用交换机流量统计策略或抓包等方式判断丢包发生的准确位置，确认是否防火墙造成；然后再依次对防火墙的端口状态、CPU/内存、配置等进行检查；如果防火墙出现临时性丢包，则应重点检查在发生丢包时，会话表项统计及快速转发统计，如果这些统计值出现异常，往往是由于突发性的异常流量短时间内在防火墙上创建了大量无用会话表项，影响了防火墙转发性能导致，通过合理地优化配置或消除攻击源即可解决。

2. 流程图相关操作说明

(1) 是否本防火墙丢包

通常情况下，丢包类问题是网络工程师利用 ICMP ping 测试发现的。在现场条件允许的前提下，建议对 ping 测试的数据包实施流量统计，以明确丢包问题是否发生在本防火墙设备上。安全产品目前不支持流量统计功能，因此需要在相连的上下行交换机端口上进行操作，防火墙插卡可以直接在宿主路由交换主机与防火墙单板的内联接口上进行操作。对于无法在路由交换设备上实施流量统计的组网情形，可以通过在流量入/出防火墙的端口位置抓包，通过对比进入防火墙之前和经过防火墙之后的报文情况来判断数据包经防火墙转发后，是否出现了丢包、乱序等异常现象。

命令：*acl number xxxx*

rule x permit icmp source x.x.x.x 0 destination x.x.x.x 0

traffic classifier xxxx

if-match acl xxxx

traffic behavior accounting

qos policy accounting

classifier xxxx behavior xxxx

qos apply policy xxxx inbound

qos apply policy xxxx outbound

display qos policy interface xxxx

例如：通过在宿主交换机与防火墙插卡的内联接口 Ten5/0/1 双方向配置流量统计策略，可以观察 10.0.0.1(客户端)与 172.16.0.1(服务器)之间的 ping 报文在经过防火墙转时，是否存在丢包。具体配置方法为先创建两条 ACL，分别匹配正反方向的 ICMP 报文，然后配置流量统计策略，应用在内联口上。注意，要对上行方向经过防火墙前/后，以及下行方向经过防火墙前/后的报文分别进行统计，这样不仅可以一次性判断防火墙是否有丢包，还可以判断在哪个方向上存在丢包。注意，ACL 规则的配置必须精确，否则会使统计策略匹配无关报文，影响统计结果和问题判断。

```
#
[H3C] acl number 3001
[H3C-acl-adv-3001] rule 5 permit icmp source 10.0.0.1 0 destination 172.16.0.1 0
#
[H3C] acl number 3002
[H3C-acl-adv-3002] rule 5 permit icmp source 172.16.0.1 0 destination 10.0.0.1 0
#
[H3C] traffic classifier client_to_server
[H3C-classifier-client_to_server] if-match acl 3001
#
[H3C] traffic classifier server_to_client
[H3C-classifier-server_to_client] if-match acl 3002
#
[H3C] traffic behavior accounting
[H3C -behavior-accounting] accounting
#
[H3C] qos policy accounting
[H3C-qospolicy-accounting] classifier client_to_server behavior acc
[H3C-qospolicy-accounting] classifier server_to_client behavior acc
#
[H3C-Ten-GigabitEthernet5/0/1] qos apply policy accounting inbound
[H3C-Ten-GigabitEthernet5/0/1] qos apply policy accounting outbound
```

流量统计策略配置完成后，再次进行 ping 测试，然后查看统计结果。通过对比双向的报文收发统计，就可以判断总共发送至防火墙多少个报文，从防火墙转发回交换机多少个报文。如果从防火墙接收的报文个数少于发送至防火墙的报文个数，则说明本防火墙确实存在丢包。如果防火墙未丢包，但 ping 发起方至 ping 响应方统计到的报文个数少于 ping 操作的报文数，则可以判断丢包是出现在 ping 发起方与防火墙之间的某个位置；反之，则丢包是出现在 ping 响应方与防火墙之间的某个位置。

如示例所示，从客户端向服务器端总共 ping 10 次，ping 测试结果显示通了 9 次，1 次超时。交换机上的流量统计策略结果显示，正方向 10 个报文全部转发给了防火墙，并且从防火墙接收到 10 个报文；而反方向交换机仅向防火墙转发了 9 个报文，并且从防火墙也接收到了 9 个报文。该结果证明，网络中确实存在丢包问题，但不是防火墙引起的；更进一步地，可以初步判断丢包是发生在服务器与防火墙之间的某个位置上。

```
<H3C> display qos policy interface Ten-GigabitEthernet 5/0/1

  Interface: Ten-GigabitEthernet5/0/1

  Direction: Inbound

  Policy:accounting
   Classifier: client_to_server
     Operator: AND
     Rule(s) : If-match acl 3001
     Behavior: accounting
      Accounting Enable:
        10 (Packets)
 Classifier: server_to_client
     Operator: AND
```

```
      Rule(s) : If-match acl 3002
      Behavior: accounting
       Accounting Enable:
         9 (Packets)

  Direction: Outbound

    Policy:accounting
      Classifier: client_to_server
      Operator: AND
      Rule(s) : If-match acl 3001
      Behavior: accounting
       Accounting Enable:
         10 (Packets)
  Classifier: server_to_client
      Operator: AND
      Rule(s) : If-match acl 3002
      Behavior: accounting
       Accounting Enable:
         9 (Packets)
```

(2) 排查其他设备问题

若确认丢包问题不是本防火墙引起,应进一步排查其他设备问题。判断丢包发生的具体位置及方向仍可参考步骤(1)中提供的思路及方法。建议采用分段排查法,逐步缩小范围。如果最终定位丢包确由非 H3C 品牌设备引起,建议及时联系相应的技术服务团队分析处理。

(3) 检查设备端口状态统计

检查防火墙端口物理层、链路层状态是否正常,检查端口的速率、双工协商状态,注意同时检查对端接口的相关属性是否与本端协商一致。检查端口出方向队列是否发生拥塞、是否出现错包等。若端口状态异常或入方向错包统计持续增加,应优先检查物理线路是否存在故障,建议通过替换法进行对比测试。

命令:*display interface interface-type interface-number*

例如:在 CLI 界面下检查防火墙端口 GigabitEthernet 0/1 的状态和统计信息。

```
<H3C> display interface GigabitEthernet 0/1
GigabitEthernet0/1 current state: Up
Line protocol current state: Up
Description: GigabitEthernet0/1 Interface
The Maximum Transmit Unit is 1500
Internet Address is 10.255.255.13/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e280-de8e
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e280-de8e
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queuing : Size/Length/ Discards)  0/100/ 0
Output queue : (Protocol queuing : Size/Length/ Discards)  0/500/ 0
Output queue : (FIFO queuing : Size/Length/ Discards)  0/75/ 0
    Last clearing of counters: Never
    Last 300 seconds input rate 43 bytes/sec, 344 bits/sec, 0 packets/sec
    Last 300 seconds output rate21 bytes/sec, 110 bits/sec, 0 packets/sec
```

```
Input: 2375264 packets, 0 jumboes, 151311918 bytes, 2375264 buffers
        272229 broadcasts, 6757 multicasts, 0 pauses
        0 errors, 0 runts, 0 giants
        0 crc, 0 align errors, 0 overruns
        0 dribbles, 0 drops, 0 no buffers
Output:17451 packets, 7045543 bytes, 17451 buffers
        2 broadcasts, 0 multicasts, 0 pauses
        0 errors, 0 underruns, 0 collisions
        0 deferred, 0 drops, 0 lost carriers
```

（4）检查 CPU/内存利用率

检查设备 CPU/内存利用率，确认设备是否出现业务繁忙。若 CPU 利用率持续超过20%，可参考安全云图——CPU 利用率高进行排查。同理，对于内存高问题可参考安全云图——内存利用率高进行排查。

命令：*display cpu-usage*

display memory

例如：在 CLI 界面下查看 CPU/内存利用率。

```
<H3C> display cpu-usage
Unit CPU usage:
      7% in last 5 seconds
      4% in last 1 minute
      3% in last 5 minutes

<H3C>display memory
System Total Memory(bytes): 3200233280
Total Used Memory(bytes): 947455312
Used Rate: 29%
```

H3CComware V5 平台防火墙基于多核多线程硬件架构设计，可通过高级命令查看到各CPU 硬件线程的负载情况。通常情况下各硬件线程负载相对平均。如果发现某个 CPU 线程负载始终远高于其他线程，则很可能是由于网络中存在单个流量较大的异常会话，当这条流量调度至该线程处理后造成其负载过大，超过了单个 CPU 线程的处理能力。针对这种情况，比较有效的方法是通过抓包等手段先查看具体的异常流量，判断其来源，然后再通过黑名单、域间策略、攻击防范、路由交换设备上的包过滤策略等手段屏蔽该流量；如果异常流量来源自内网，建议直接找出并消除攻击源。

命令：*tshow mainboard cpu-usage all*

例如：在 CLI 界面下查看 CPU 各硬件线程负载情况。在本例中 13 号线程负载持续达到99%，说明该线程负载过大，经抓包确认防火墙端口持续接收到大流量重复的 ARP 报文，进一步对网络进行排查时发现防火墙下联二层网络存在环路，于是产生了 ARP 报文风暴。二层环路复制产生的报文全部相同，因此在 CPU 多核调度时都上送了单个硬件线程处理，这时如果还有其他普通业务报文也调度至该硬件线程时便会出现丢弃问题。

```
[H3C_hidecmd]tshow mainboard cpu-usage all
  VCPU usage information:
   1    3%
   2    4%
   3    5%
```

```
4   4%
5   4%
6   4%
7   5%
8   6%
9   3%
10  3%
11  4%
12  3%
13  99%
14  5%
15  3%
```

(5) 检查虚拟分片重组

若 ping 测试结果显示设备可以正常转发一般长度 IP 报文(小于 1500 字节),随机丢弃大报文(大于 1500 字节),设备同时上报 IP 分片攻击日志(atckType=Frag Flood),这时应检查虚拟分片重组功能是否已经启用,配置参数是否合理。默认情况下每个安全区域可同时处理 64 个 IP 大包,每个报文最多可以分 16 个分片,重组时限为 3 秒。根据以太网类型链路 MTU 1500 字节粗略计算,防火墙默认配置下可以转发长度为 1500×16=24000 字节的 IP 包,更大的 IP 包会判定为分片攻击并被防火墙丢弃处理。在多数场景中,可以将虚拟分片重组功能的"分片队列数"调整至 1024,将"分片报文数"调整至 64,老化时间保持不变,然后再进行测试确认。这类问题通常是工程师 ping 大包测试时发现的,而一般的业务流通常是 TCP 或 UDP 协议承载,TCP 业务可以通过调整 TCP MSS 参数控制报文不在 IP 层进行分片操作,UDP 业务通常都是小包也不会在 IP 层进行分片,所以通常不涉及。如果网络中存在 IPSec 业务流,应当注意进行调整,避免 IPSec 封装后的报文超过 MTU 值在 IP 层分片后,由于防火墙虚拟分片重组功能而丢弃。

命令:*ip virtual-reassembly max-fragments xxx max-reassemblies xxxx*

例如:在 CLI 界面下,进入 Untrust 区域视图,使能虚拟分片重组功能配置并调整参数。Web 配置界面中也可以进行相关配置及参数修改。

```
[H3C] zone name Untrust
[H3C-zone-Untrust] ip virtual-reassembly max-fragments 64 max-reassemblies 1024
```

(6) 检查会话统计

防火墙从业务端口接收到报文后,会利用防火墙会话表项对该报文是否符合协议状态机、是否为域间策略所允许等进行一系列检查,对检查不通过的报文将丢弃处理。在正常运行过程中,防火墙会不断地新建会话表项和保持会话表项,如果防火墙在会话表项老化时间内,始终没有再接收到双向业务报文时还会主动删除该会话表项。在防火墙的会话表统计信息中,网络管理员可以查看到本防火墙的新建连接速率、当前并发连接总数、接收报文统计、丢弃报文统计等。通过将新建连接速率、当前并发连接总数与日常运维过程中所观察记录的数据做对比,可以判断防火墙是否正在受到异常流量攻击,是否创建了大量的无效会话。

命令:*display session statistics*

例如:某防火墙在正常运行过程中,管理员通过命令观察到会话统计信息如下所示。其中,会话表项总数为 4.7 万,TCP 连接 8159 个,半开连接 1757 个;防火墙会话表项每秒新建约 1600 个,各项数据符合预期,实际网络业务运行正常。

```
<H3C> display session statistics
Current session(s):47197
          Current       TCP session(s): 8159
                    Half-Open: 1757           Half-Close: 807
          Current       UDP session(s): 36984
          Current      ICMP session(s): 2054
          Current     RAWIP session(s): 0

Current relation table(s): 3

Session establishment rate:          1641/s
          TCP       Session establishment rate:          660/s
          UDP       Session establishment rate:          915/s
          ICMP      Session establishment rate:           66/s
          RAWIP     Session establishment rate:            0/s

Received        TCP:    2961011924 packet(s)       1967012350403 byte(s)
Received        UDP:    8143088477 packet(s)       4811797756742 byte(s)
Received       ICMP:     117875937 packet(s)          7833600288 byte(s)
Received      RAWIP:       1546303 packet(s)           225944006 byte(s)
Dropped         TCP:     146473628 packet(s)          5965991706 byte(s)
Dropped         UDP:       4667609 packet(s)           503717261 byte(s)
Dropped        ICMP:      18230886 packet(s)          1855796027 byte(s)
Dropped       RAWIP:            52 packet(s)                4573 byte(s)
```

在某时间点用户反馈网络突然出现丢包问题，通过命令观察到如下所示的会话统计信息。其中，会话总数已经激增到135.8万，其中TCP连接132万，而TCP半开连接就有131万，TCP半开连接比率高达99.3%；此时防火墙会话表项每秒新建连接数也达到6.5万，远远高于日常观察值。从以上信息可以判断，目前网络中存在典型的TCP SYN Flood攻击流量。针对这类攻击，可以先利用当前设备的会话表项详细信息来分析特点和来源，如果攻击是来源于网络外部或Internet的，一般通过启用攻击防范手段来防御，方法包括黑名单、域间策略、流量异常检测等；如果攻击是来源于网络内部的，最好的方法就是直接找到这个内部攻击源并消除。

```
<H3C> display session statistics
Current session(s):1358079
          Current       TCP session(s):1324027
                    Half-Open:1315375           Half-Close: 1455
          Current       UDP session(s): 33995
          Current      ICMP session(s): 57
          Current     RAWIP session(s): 0

Current relation table(s): 9

Session establishment rate:        65172/s
          TCP       Session establishment rate:        63640/s
          UDP       Session establishment rate:         1522/s
          ICMP      Session establishment rate:           10/s
          RAWIP     Session establishment rate:            0/s
```

```
Received      TCP:    2945317802 packet(s)    1963716576218 byte(s)
Received      UDP:    8133194950 packet(s)    4806408621655 byte(s)
Received     ICMP:     117822713 packet(s)       7829261947 byte(s)
Received    RAWIP:       1546250 packet(s)        225938755 byte(s)
Dropped       TCP:     145438758 packet(s)       5924334398 byte(s)
Dropped       UDP:       4642510 packet(s)        500942861 byte(s)
Dropped      ICMP:      18230740 packet(s)       1855789890 byte(s)
Dropped     RAWIP:            52 packet(s)             4573 byte(s)
```

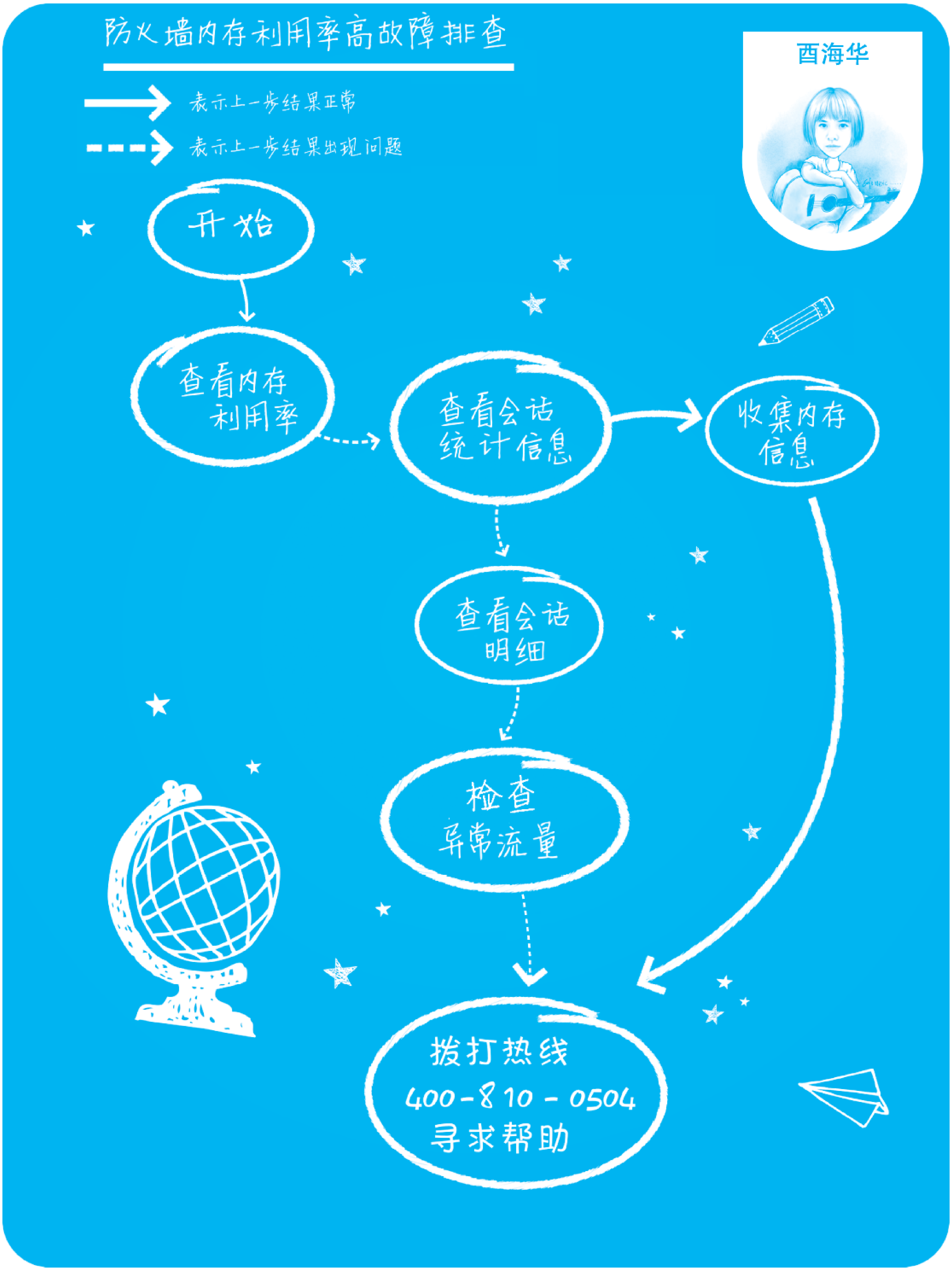
（7）检查快速转发

H3CComware V5 平台防火墙支持报文快速转发特性。当防火墙接收到业务报文后，将优先通过快速转发处理；不支持快速转发的业务流再按照普通流程处理。防火墙快速转发状态统计中，包括是否已经启用快速转发功能等非常详细的相关信息。在进行丢包问题排查时，主要关注的统计项为“Forward packets”——经快速转发处理的报文个数；“Up packets”——经普通流程转发的报文个数；“Up failed packets”——转发丢弃的报文个数。如果“Up failed packets”计数增长较快，可以尝试对防火墙实施配置优化，以期让更多的业务报文经快速转发流程处理来提高性能。主要的优化方法包括：关闭不使用的 ALG 协议模块、取消不必要的 QoS 策略、减少频繁的 ARP 和路由表项振荡、配置目的安全区域为 Local 的阻断域间策略（注意允许管理流量通过）以加固防火墙自身安全、调短会话表项生存时间以加快无效会话的老化删除等。

命令：*display ip fast-forwarding statistics*

例如：通过命令查看当前设备快转状态，其中经快速转发处理报文 12339 个，普通转发流程处理报文 1056 个，没有出现转发丢弃报文。

```
[H3C-hidecmd] display ip fast-forwarding statistics
Ip fast-forwarding state : enable
  Ip fast-forwarding enable
--------------------------------------------------
  Sum statistics
  Forward    packets          12339
  Up packets                  1056
  Up failed packets           0
  Up redirect packets         0
  Forward redirect packets    0
  TTL error packets           0
  Bad checksum                0
  Bad IP head len             0
  Bad len                     0
  Hardware dropped packets    0
  Software dropped packets    0
  Create session              0
  …
```


防火墙内存利用率高故障排查
表示上一步结果正常
表示上一步结果出现问题
西海华
开始
查看内存利用率
查看会话统计信息
收集内存信息
查看会话明细
检查异常流量
拨打热线
400-810-0504
寻求帮助

1. 开始

内存利用率高是防火墙最常见的问题之一，防火墙会话是占用内存的主要模块，所以定位内存利用率高的问题要重点关注防火墙的会话及流量等信息。防火墙内存利用率高问题定位故障的思路是：首先查看会话总数是否正常，如果会话总数太多可能是因为流量太大或者存在攻击，此时可以通过抓包或者查看会话等手段查找异常的流量并进行相应处理；如果会话数不多但占用率依然很高，有可能是内存碎片过多或者挂死无法释放等问题，需要收集设备内存详细信息进一步分析定位。

2. 流程图相关操作说明

（1）查看内存利用率

命令：*display memory*

一般情况内存使用率建议不高于70%，如果持续高于70%，需要引起关注。

```
[H3C]display memory
System Total Memory(bytes): 1874838960
Total Used Memory(bytes): 1048363440
Used Rate: 55%
```

（2）查看会话统计信息

如果防火墙收到异常流量或者网络存在攻击，会话统计信息会有明显异常，例如会话总数、半开连接数以及会话新建速率等参数都会明显高于正常值，所以查看会话统计的时候要重点关注这几个参数。

命令：*display session statistics*

例如：网络受到SYN-Flood攻击，TCP连接总数和连接速率都明显偏高，而且大部分TCP连接都是半开连接。

```
[H3C]display session statistics
Current session(s):2959981
         Current      TCP session(s): 2827396
                  Half-Open: 2765555       Half-Close: 24194
         Current      UDP session(s): 132052
         Current     ICMP session(s): 532
         Current    RAWIP session(s): 1

Current relation table(s): 14

Session establishment rate:       60815/s
         TCP       Session establishment rate:       59599/s
         UDP       Session establishment rate:        1207/s
…
```

（3）查看会话明细

防火墙的会话记录了经过防火墙的每一条数据流的详细信息，查看会话明细的时候重点关注源目地IP和端口、安全域间、会话状态和双向收发报文计数。根据会话详细信息，可以初

步判断网络中是否有异常流量，以及异常流量的 IP 地址、端口等信息。

命令：*display session table verbose*

例如：通过命令可以看到当前防火墙上有一条 10.0.0.1 到 10.255.255.43 的数据流，协议是 TCP，具体应用是 Telnet，会话的状态是 TCP-EST，报文的源域是 Untrust，目的域是 Trust，收发报文都正常。

```
[H3C]display session table verbose
Initiator:
  Source IP/Port : 10.0.0.01/5420
  Dest IP/Port   : 10.255.255.43/23
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 10.255.255.43/23
  Dest IP/Port   : 10.0.0.1/5420
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)     App: TELNET            State: TCP-EST
Start time: 2013-05-03 13:28:40   TTL: 3600s
Root                         Zone(in): Untrust
                             Zone(out): Trust
Received packet(s)(Init): 32 packet(s) 1346 byte(s)
Received packet(s)(Reply): 30 packet(s) 1785 byte(s)
```

(4) 检查是否存在异常流量

进一步查看会话详细信息，可以初步判断网络中是否有异常流量，以及异常流量的 IP 地址、端口等信息。可以通过查看多条会话详细信息查找规律，另外还可以通过抓包的方式查看异常流量的信息。

命令：*display session table verbose*

例如：通过命令查看多条详细会话信息，受到 SYN Flood 攻击的设备会话详细有如下特点：会话状态 SYN，一般目的 IP 比较固定，大多数情况是内部的服务器，反向可能没有回包。

另外除攻击流量外还可能防火墙外部环路或者内部环路使得并发较高，这类报文显著特点是进出区域相同，结合正常路由判断进出区域判断是否正常。如果不能单从会话信息判断故障，可以考虑在防火墙前后抓包分析。

```
[h3c]display session table verbose
Initiator:
  Source IP/Port : 255.91.195.14/26851
  Dest IP/Port   : 115.239.230.214/7444
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 115.239.230.214/7444
  Dest IP/Port   : 255.91.195.14/26851
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: unknown       State: SYN
Start time: 2013-04-18 03:35:46   TTL: 0s
Root                           Zone(in):Untrust
                               Zone(out):Trust
Received packet(s)(Init): 1 packet(s) 40 byte(s)
Received packet(s)(Reply): 0 packet(s) 0 byte(s)
Initiator:
```

```
    Source IP/Port : 137.114.132.16/25480
    Dest IP/Port    : 115.239.230.214/7444
    VPN-Instance/VLAN ID/VLL ID:
  Responder:
    Source IP/Port : 115.239.230.214/7444
    Dest IP/Port    : 137.114.132.16/25480
    VPN-Instance/VLAN ID/VLL ID:
  Pro: TCP(6)        App: unknown         State: SYN
  Start time: 2013-04-18 03:36:04    TTL: 1s
  Root                              Zone(in):
                                    Zone(out):
  Received packet(s)(Init): 1 packet(s) 40 byte(s)
  Received packet(s)(Reply): 0 packet(s) 0 byte(s)
```

（5）收集内存信息

如果防火墙的会话信息正常，但是内存利用率还是比较高，可以收集地址池详细分配信息，反馈给二线进一步分析。另外最好把诊断信息和设备配置文件也一起收集。

命令：_*display memory*

_*display memory-pool*

_*display memory raw all partition 0*

_*display memory raw all core 0*

例如：通过_*display memory-pool* 命令可以查看具体哪些模块占用内存过多，此处按照以上命令顺序执行记录设备输出信息即可。

```
[h3c]_h
[H3C-hidecmd]_display memory-pool
name index csize freenum  totalnum bnum   align cacheflag tableAddr    tablesize
-----------------------------------------------------------------------------------
SETB  22     380    2699      2716      1       32     0x7          0x1b19348    8
SENG 23      20     30821     30838     1       32     0x7          0x1c03c28    8
...
```


防火墙双机热备故障排查
西海华
表示上一步结果正常
表示上一步结果出现问题
开始
查看双机热备状态
查看配置同步状态
检查配置
检查版本和配置
查看物理链路
拨打热线
400-810-0504
寻求帮助

1. 开始

防火墙的双机热备功能可以实现会话和配置的同步，从而简化配置并且提高网络的可靠性。防火墙双机热备问题定位故障的思路是：首先检查防火墙双机热备状态是否是同步运行，如果不是同步状态，请检查两台防火墙的版本是否一样、双机热备配置是否正确以及双机热备链路是否正常；状态同步后再检查配置同步状态，如果存在配置冲突，最好将备机的 Web 配置清除，然后再从主机同步配置。

2. 流程图相关操作说明

(1) 查看双机热备状态

进入主备两台防火墙 Web 页面，单击"高可靠性"→"双机热备界面"，如图 6-54 所示，查看双机热备状态，如果显示"同步运行"则状态正常。



图 6-54 双机热备配置(1)

关于热备状态的说明。

① 静默：表示设备刚启动正在等待系统稳定，或者热备状态正在从同步运行向独立运行转换的中间状态。

② 独立运行：表示静默定时器超时，但是设备没有与任何其他设备建立备份连接。

③ 同步运行：表示设备与对端设备状态协商成功，状态达到同步。

(2) 检查版本和配置

双机热备设备版本需要一致，如果两台防火墙双击热备状态无法同步，首先检查设备版本，然后再检查双击热备相关配置。

命令：*display version*

例如：通过命令查看，可以确认两端版本是否一致。

```
[H3C]display version
H3C Comware Platform Software
Comware Software, Version 5.20, Feature 3171P08
Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C SecPath F1000-E uptime is 1 week, 1 day, 11 hours, 25 minutes
```

然后再进入防火墙 Web 页面，单击"高可靠性"→"双机热备界面"，如图 6-55 所示，确认两台设备双击热备配置一致。



图 6-55　双机热备配置(2)

① 使能会话双机热备功能：可以实现 NAT、ALG、ASPF 业务会话的备份，必配。

② 使能 ipsec 双机热备功能：可以实现 ipsec 会话的备份，按需配置。

③ 使能支持非对称路径：开启该功能后，可以保证一条会话中的数据流进入内网和从内网出去所经过的设备不同时，业务不受影响，推荐配置。

④ 备份接口：确保配置相同的接口，如果有 2 个接口，配置顺序需要相同，推荐直连，必配。

⑤ 备份 VLAN：当两台防火墙备份口不是直连而是通过交换机等设备相连时，需要通过 VLAN 传送心跳报文。确保设备 VLAN 配置相同，再查看中间交换机上是否传送备份 VLAN。

(3) 查看物理链路

查看双机热备的心跳链路是否正常。

命令：*display interface interface-type interface-number*

例如：查看端口是否 Up，物理链路是否正常。

```
[H3C]display interface GigabitEthernet 0/4
GigabitEthernet0/4 current state: Up
Line protocol current state: Up
Description: GigabitEthernet0/4 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e27c-7798
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e27c-7798
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last clearing of counters: Never
    Peak value of input: 718 bytes/sec, at 2013-12-24 10:54:48
    Peak value of output: 3034 bytes/sec, at 2013-12-24 10:54:48
    Last 300 seconds input rate 544 bytes/sec, 4352 bits/sec, 7 packets/sec
    Last 300 seconds output rate 544 bytes/sec, 4352 bits/sec, 7 packets/sec
    Input: 445307 packets, 0 jumboes, 34609502 bytes, - buffers
           445307 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 runts, 0 giants
           0 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
```

```
Output:445477 packets, 34634050 bytes, - buffers
        445477 broadcasts, 0 multicasts, 0 pauses
        0 errors, 0 underruns, 0 collisions
        0 deferred, 0 drops, 0 lost carriers
```

(4) 查看配置同步状态

进入防火墙 Web 页面,单击“高可靠性”→“双机热备界面”,如图 6-56 所示,查看当前设备的配置同步状态是否正常。



图 6-56 双机热备配置(3)

例如:通过 Web 查看双机热备状态,显示同步运行。

① 配置冲突:两台设备均为主设备或者备设备,或者主备设备配置存在冲突。

② 等待同步运行状态:等待双机热备进入同步运行状态。

③ 准备同步:准备将主设备当前配置同步到备设备。

④ 同步所有配置中:启用了自动同步更新配置功能,主设备正在将当前配置同步到备设备。

⑤ 自动同步更新配置:启用了自动同步更新配置功能,两台设备已经完成了同步所有配置的过程。

⑥ 不进行自动同步:没有启用自动同步更新配置功能。此时,用户在主设备上的配置操作不会自动同步到备设备上。

(5) 检查配置

进入防火墙 Web 页面,单击“高可靠性”→“双机热备界面”,如图 6-57 所示。检查主备防火墙配置同步功能配置是否正确。

主设备配置如图 6-57 所示。



图 6-57 主设备配置

备设备配置如图 6-58 所示。



图 6-58　备设备配置

启用自动同步更新配置后，当前主设备上支持配置同步功能的配置将同步到备设备上，且后续用户在主设备上的配置操作也会自动同步到备设备上。

该配置只需要在配置同步的主设备上配置。

防火墙配置同步的内容主要包括以下内容。

① 设备管理：安全域、虚拟设备、服务管理。

② 资源管理：地址、服务、时间段。

③ 防火墙：安全策略、NAT 映射、ALG、ACL、会话管理。

④ 攻击防范：黑名单、报文异常检测、流量异常管理、URPF 检查、TCPProxy。

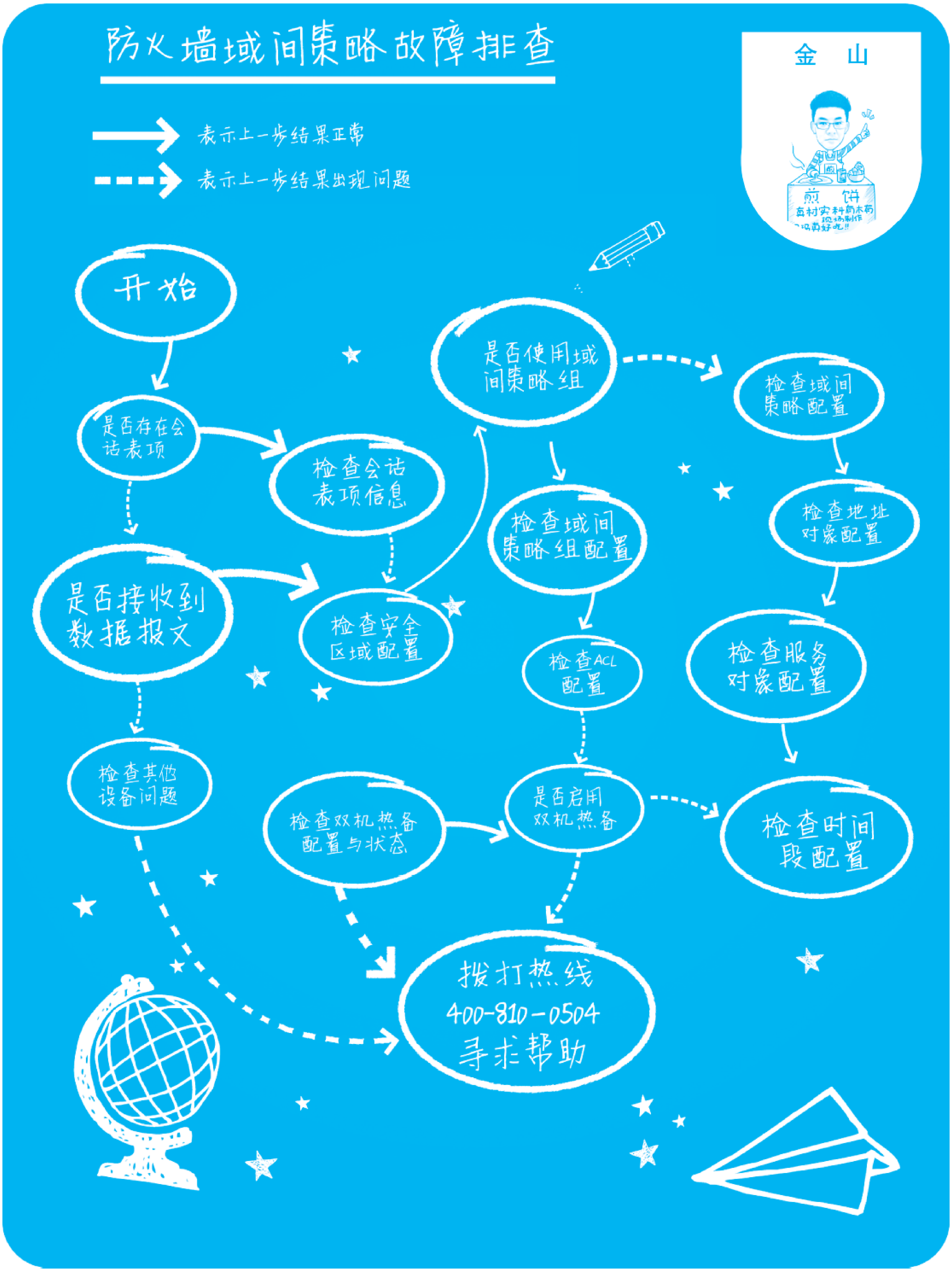
⑤ 应用控制：内容过滤。

⑥ VPN：IKE、IPSec。

⑦ 高可靠性：使能双机设备、使能 IPSec 双机热备、作为配置同步的主设备。

⑧ 日志管理：Syslog、Userlog、会话日志、命令行配置同步。

当两台设备配置已经发生不同步或者配置冲突时，需要清空备设备 Web 界面的配置，然后开启双机热备，使主设备上的配置自动同步到备设备上。


防火墙域间策略故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
煎 饼
开始
是否存在会话表项
检查会话表项信息
是否接收到数据报文
检查安全区域配置
检查其他设备问题
是否使用域间策略组
检查域间策略组配置
检查ACL配置
是否启用双机热备
检查双机热备配置与状态
检查域间策略配置
检查地址对象配置
检查服务对象配置
检查时间段配置
拨打热线
400-810-0504
寻求帮助

1. 开始

防火墙域间策略问题定位故障的思路是：首先在防火墙上查看业务流所对应的会话表项是否存在。若会话表项存在，则需要仔细检查会话表项所包括的源/目的安全区域、发起/响应方五元组、协议状态等信息是否符合预期，否则应按域间策略的正常配置顺序检查防火墙是否存在配置错误。若防火墙上虽然可以查询到会话表项，但没有响应方报文统计，这种情况很可能是由于路由交换网络未能将会话反向报文正确转发至本防火墙造成的，此时需要从整网角度，尤其是报文转发路径方面着手排查。若防火墙上业务流对应的会话表项不存在，一种可能是由于业务报文被域间策略阻断而未能创建会话，这种情况需要重点检查阻断动作的域间策略是否配置正确；另一种可能是防火墙确实没有接收到会话发起方相应的业务报文，这种情况通常需要排查网络中防火墙上游其他设备是否存在转发故障。域间策略是 H3C Comware V5 平台防火墙非常稳定的基础安全特性，无论现场遇到的问题是“应该通的没通”还是“不应该通的通了”，相信通过确认组网连接、检查设备配置、观察业务报文收发情况、观察防火墙会话表项信息等一系列排查手段，最终都能得到定位和解决。

2. 流程图相关操作说明

(1) 是否存在会话表项

H3C Comware V5 平台防火墙属于状态检测防火墙，会话表项是防火墙对网络中各条业务流执行状态检测的重要依据。防火墙从某业务端口接收报文后，与当前会话表进行匹配。如果报文命中某条会话表项，意味着可以继续转发。如果无法命中任何会话表项，该报文将转交给域间策略模块进行策略匹配，匹配结果为允许，防火墙将创建一条新的会话表项并转发该报文；匹配结果为拒绝则丢弃该报文且不创建会话。

为了更精确地查找会话表项，防火墙支持基于会话发起方的源/目的 IP 地址、源/目的端口号、协议、虚拟设备名称等参数执行筛选查找。要注意执行命令的时机必须在会话老化以前，以 UDP、ICMP 协议会话为例，如果防火墙没有接收到后续命令会话的业务报文，则该会话会在 60 秒后删除。若查询命令执行后显示会话表项数为 0，说明当前不存在符合查询条件的会话表项。

命令：*display session table source-ip x.x.x.x destination-ip x.x.x.x verbose*

例如：网络管理员执行 5 次 ping 操作，会话发起方源/目的地址分别为 10.0.20.2/10.0.30.2，ping 报文经过防火墙时命中允许动作域间策略，因此在会话表中可以查询到如下表项，会话发起方为 10.0.20.2，会话响应方为 10.0.30.2，发起方位于 Untrust 区域，响应方位于 Trust 区域，发起方发送了 5 个报文，响应方回复了 5 个报文。若防火墙没有收到后续报文，会话将在 9 秒后删除。

```
[H3C]display session table source-ip 10.0.20.2 destination-ip 10.0.30.2 verbose
Initiator:
  Source IP/Port : 10.0.20.2/2048
  Dest IP/Port   : 10.0.30.2/14422
```

```
    VPN-Instance/VLAN ID/VLL ID:
  Responder:
    Source IP/Port : 10.0.30.2/0
    Dest IP/Port   : 10.0.20.2/14422
    VPN-Instance/VLAN ID/VLL ID:
  Pro: ICMP(1)    App: unknown          State: ICMP-CLOSED
  Start time: 2013-12-17 17:45:08 TTL: 9s
  Root                     Zone(in): Untrust
                           Zone(out): Trust
  Received packet(s) (Init): 5 packet(s) 420 byte(s)
  Received packet(s) (Reply): 5 packet(s) 420 byte(s)

   Total find: 1
```

（2）是否接收到数据报文

若防火墙上业务流对应的会话表项不存在，一种可能是由于业务报文被域间策略阻断而未能创建会话，这种情况需要重点检查阻断动作的域间策略是否配置正确；另一种可能是防火墙确实没有接收到会话发起方相应的业务报文，这种情况通常需要排查网络中防火墙上游其他设备是否存在转发故障。为了区别这两种不同的可能性，需要通过 debugging 命令的输出信息来协助判断。在使能 debugging 开关时必须引用精确匹配业务报文的 ACL 过滤输出，避免大量的无效信息干扰分析。

命令：*debugging ip packet acl xxxx*

debugging firewall packet-filter xxxx acl xxxx

例如：如下所示，先配置 ACL 规则用于精确匹配 ping 测试的流量，发起方源/目的 IP 地址分别为 10.0.20.2/10.0.30.2，然后打开 debugging 开关，接着再重新操作 ping 操作，最后观察 debugging 命令的输出信息：防火墙接收并尝试路由转发了这个 ICMP 包，但随后在进行域间策略查找匹配时，被源域为 Untrust 目的域为 Trust 的阻断规则丢弃，ACL none 表示该报文命中了默认域间规则，即默认的低优先级安全区域不能主动访问高优先级安全区域。

```
  [H3C] acl number 3001
  [H3C-acl-adv-3001] rule 5 permit icmp source 10.0.20.2 0 destination 10.0.30.2 0

  <H3C> debugging ip packet acl 3001
  <H3C> debugging firewall packet-filter icmp acl 3001

  <H3C> terminal debugging
  Info: Current terminal monitor is on.
  <H3C> terminal monitor
  Info: Current terminal debugging is on.

  <H3C>
  *Dec 18 09:16:27:080 2013 SecBladeII_3 DPIPFWD/7/debug_case:
  Receiving, interface = Ten-GigabitEthernet0/0.20, version = 4, headlen = 20, tos = 0,
  pktlen = 84, pktid = 39142, offset = 0, ttl = 255, protocol = 1,
  checksum = 56510, s = 10.0.20.2, d = 10.0.30.2
```

```
prompt: Receiving IP packet

 * Dec 18 09:16:27:081 2013 SecBladeII_3 DPIPFWD/7/debug_case:
Sending, interface = Ten-GigabitEthernet0/0.30, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 39142, offset = 0, ttl = 254, protocol = 1,
checksum = 56766, s = 10.0.20.2, d = 10.0.30.2
prompt: Sending the packet from Ten-GigabitEthernet0/0.20

 * Dec 18 09:16:27:081 2013 SecBladeII_3 FILTER/7/debug:
 Thread 23, the icmp packet is denied from Untrust to Trust: (10.0.20.2)->(10.0.30.2), 84 bytes,
ACL none.
```

(3) 检查其他设备问题

若防火墙没有接收到业务报文，则问题很可能发生在发起方至防火墙之间的某个位置，可能是由于组网、路由规划、其他设备故障等因素导致报文没有到达或者绕过防火墙。建议从发起方开始逐跳排查，逐步确认报文的具体转发路径、是否存在丢包等。如确认是非 H3C 品牌设备引起的故障，应尽快与设备的服务提供商取得联系。

(4) 检查会话表项信息

在防火墙上查询到会话表项后，应根据实际组网情况核对表项信息是否符合预期。重点检查会话表项的源/目的安全区域是否正确，发起/响应方报文五元组、VLAN 等是否正确，会话正反方向上接收的报文数统计是否正确等。如果源/目的安全区域不符合预期，通常是端口安全区域属性配置错误或路由表配置错误造成。如果发起方/响应方的五元组信息不符合预期，则多见于 NAT 策略配置错误。如果防火墙在会话反方向没有接收到响应方回复的报文，则多数是业务流来回转发路径不一致，即反方向报文未经本防火墙转发造成。

命令：*display session table source-ip x.x.x.x destination-ip x.x.x.x verbose*

例如：网络管理员执行 5 次 ping 操作，发起方源/目的 IP 地址分别为 10.0.20.2/10.0.30.2。从会话表项中可以查看到发起方处于 Untrust 区域、响应方处于 Trust 区域，防火墙在会话正/反方向各处理了 5 个数据包，该会话属于 ICMP 协议类型，当前处于 ICMP-CLOSED 状态，如果没有匹配该会话的后续数据包到达本防火墙，那么这条表项将在 15 秒后老化删除。

```
[H3C]display session table source-ip 10.0.20.2 destination-ip 10.0.30.2 verbose
Initiator:
  Source IP/Port : 10.0.20.2/2048
  Dest IP/Port   : 10.0.30.2/14608
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 10.0.30.2/0
  Dest IP/Port   : 10.0.20.2/14608
  VPN-Instance/VLAN ID/VLL ID:
Pro: ICMP(1)      App: unknown          State: ICMP-CLOSED
Start time: 2013-12-18 11:23:07     TTL: 15s
Root                      Zone(in): Untrust
                          Zone(out): Trust
```

```
Received packet(s) (Init): 5 packet(s) 420 byte(s)
Received packet(s) (Reply): 5 packet(s) 420 byte(s)

 Total find: 1
```

例如：在 Web 管理界面的“防火墙→会话管理→会话列表”页签中查看会话表项的具体信息，如图 6-59 所示。

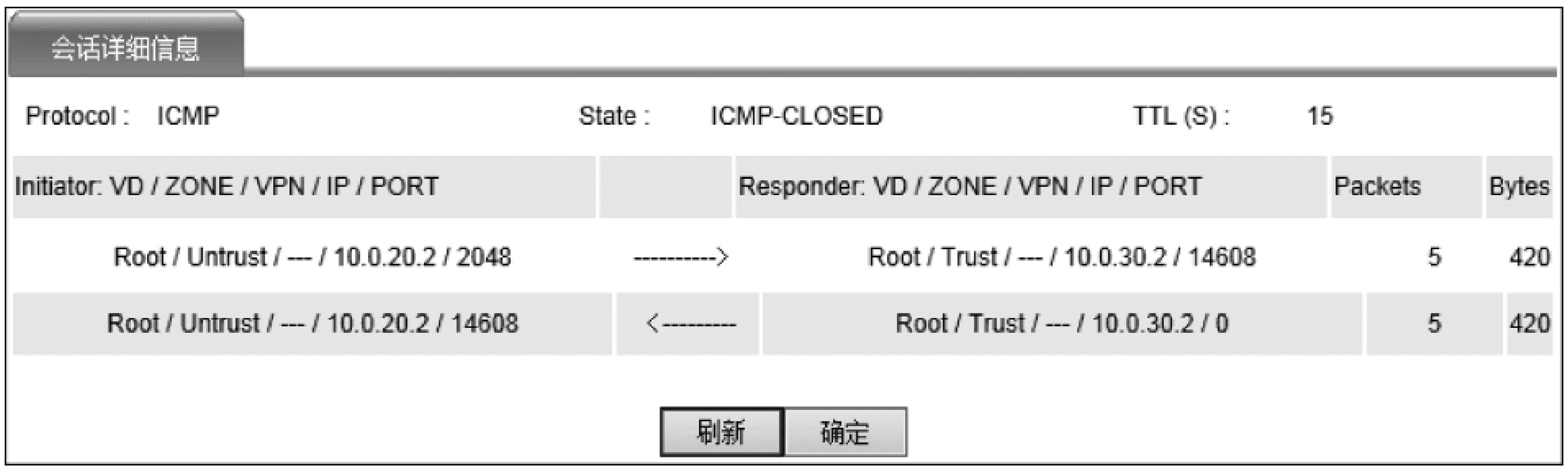


图 6-59　会话详细信息

(5) 检查安全区域配置

域间策略是防火墙在不同的源/目的安全区域之间部署的安全策略，因此必须确保各个端口添加了准确的安全区域属性。防火墙默认第一个物理端口已添加为管理区域，其他端口(包括二三层物理端口、二三聚合端口、隧道口、VLAN 虚接口、虚接口模板等)默认均无安全区域属性，必须手工配置后才能真正转发业务报文。将端口加入某个安全区域，不是指防火墙端口本身属于这个区域，而是意味着这个端口所连接的网络处于该安全区域内。虽然没有明确地体现，但切记防火墙自身全部端口都属于 Local 区域。端口的安全区域属性支持通过 CLI 或 Web 页面进行配置与查看。

命令：*display current-configuration configuration vsys*

例如：在 CLI 管理界面中，通过命令检查设备当前安全区域配置情况。其中 GigabitEthernet0/1 默认配置已加入管理区域，Ten-GigabitEthernet0/0.20 和 Ten-GigabitEthernet0/0.30 分别加入了 Untrust 区域和 Trust 区域。

```
[H3C] display current-configuration configuration vsys
#
zone name Management id 0
 priority 100
 import interface GigabitEthernet0/1
zone name Local id 1
 priority 100
zone name Trust id 2
 priority 85
 import interface Ten-GigabitEthernet0/0.30
zone name DMZ id 3
 priority 50
 share enable
zone name Untrust id 4
 priority 5
 import interface Ten-GigabitEthernet0/0.20
```

例如：在 Web 管理界面的“设备管理→接口管理”页签中，查看端口安全区域配置情况，如图 6-60 所示。在本例中防火墙通过两个三层子接口进行转发，主接口无须配置安全区域。

名称↑	IP地址	网络掩码	安全域	状态	操作
GigabitEthernet0/1	10.255.255.33	255.255.255.0	Management		
GigabitEthernet0/2			-		
GigabitEthernet0/3			-		
GigabitEthernet0/4			-		
NULL0			-		
Ten-GigabitEthernet0/0			-		
Ten-GigabitEthernet0/0.20	10.0.20.254	255.255.255.0	Untrust		
Ten-GigabitEthernet0/0.30	10.0.30.254	255.255.255.0	Trust		

共8条，每页 100 条 | 当前：1/1页，1~8条 | 首页 上一页 下一页 尾页 1 跳转

新建

图 6-60　端口安全区域配置情况

(6) 是否使用域间策略组

H3C Comware V5 平台防火墙支持域间策略组、域间策略两种配置方式。域间策略组通过将 ACL 直接应用在安全区域间实现。这种配置方法在 V5 平台防火墙替换原有网络中的包过滤防火墙时比较常用，可以实现快速移植原有 ACL 包过滤策略的目的。域间策略则通过将网络地址、端口信息抽象为地址资源、服务资源，结合时间段资源，实现基于面向对象思想的部署方式，更加灵活有效。注意，两种配置方式只能任选其一，即如果采用域间策略组方式进行安全策略配置，那么就无法再使用域间策略方式。

(7) 检查域间策略组配置

若采用域间策略组方式进行配置，应重点检查引用的 ACL 规则、引用的顺序是否准确。在 Web 管理页面中，当一条域间策略组中同时引用了多个 ACL 规则时，系统将按显示顺序(从左至右、从上至下)依次进行匹配，在 CLI 界面中同理，按显示顺序(从上至下)依次进行匹配；该显示顺序亦为管理员的策略配置顺序。此外，还应注意检查域间策略组是否已经启用。在 Web 页面中，当启用选项显示为绿包箭头向上时，表示当前处于已启用状态；反之为不生效状态。

命令：*interzone source xxxx destination xxxx*

rule acl xxxx

rule acl enable

例如：在 CLI 管理界面中，进入域间视图，检查域间策略组配置情况。在本例中，当业务流量从 Untrust 区域发起，目标为 Trust 区域时，将按照先 ACL 3001 后 ACL 3002 的顺序进行策略匹配。

```
[H3C] interzone source Untrust destination Trust
[H3C-interzone-Untrust-Trust]display this
#
interzone source Untrust destination Trust
 rule acl 3001
 rule acl 3002
 rule acl enable
#
```

在 Web 管理界面的“防火墙→安全策略→域间策略组”页签中，检查策略配置，如图 6-61 所示。当源/目的安全区域之间存在多条 ACL 策略时，按先 ACL 3001 后 ACL 3002 的顺序进行匹配。



图 6-61　策略配置

(8) 检查 ACL 配置

检查域间策略组所引用的 ACL 配置是否正确，需注意域间策略组仅关心 ACL 规则中与报文五元组相关的信息，即 IP 报文的“源/目的 IP 地址”“源/目的端口号”“协议类型”。

部分型号防火墙还支持 ACL 加速功能，若发现对应的 ACL 加速状态为“失效”，应先停止加速后再重新使能加速(该 ACL 包含规则数量大于 1K)，或停止加速(该 ACL 包含规则数量小于 1K)。

命令：*display acl xxxx*

例如：在 CLI 管理界面中，通过命令查看 ACL 规则配置是否正确。

```
<H3C> display acl 3001
Advanced ACL  3001, named -none-, 1 rule,
ACL's step is 5
rule 5 permit ip source 10.0.0.0 0.255.255.255 destination 172.16.0.0 0.15.255.255
```

在 Web 管理界面的“防火墙→ACL”页签中，检查 ACL 规则的配置情况，如图 6-62 所示。



图 6-62　ACL 规则配置

命令：*display acl accelerate all*

例如：通过命令查看 ACL 加速状态是否正常，若状态列显示为“OOD”，说明当前加速状态已失效，必须停止加速后再次重新使能。如果 ACL 内包含的规则数较少，或管理员需要经常性对规则进行增删、修改等操作，建议不要使能 ACL 加速。

```
<H3C> display acl accelerate all
 S(Status): UTD -- up to date,    OOD -- out of date
 A(Accelerate): ACC -- accelerated,   UNACC -- unaccelerated

 Group              Accelerate            Status
 ------------------------------------------------
 3001               ACC                   OOD
```

在 Web 管理界面的“防火墙→ACL”页签中，检查 ACL 的加速状态，如图 6-63 所示。在本例中，ACL3001 的加速状态为“失效”，管理员必须立即手工操作重新加速，或停止加速。

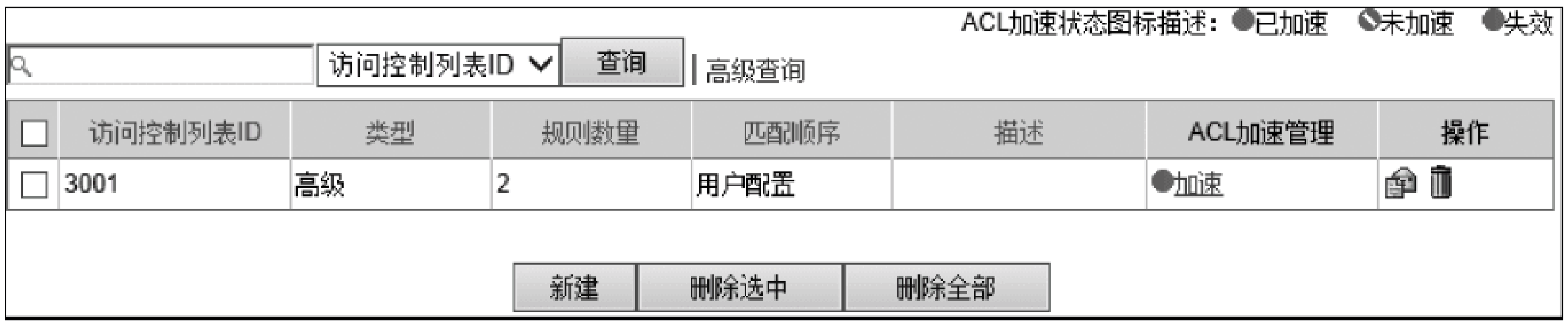


图 6-63 ACL 加速状态

（9）检查域间策略配置

检查域间策略配置是否正确，重点检查域间策略的匹配顺序是否符合客户预期。在 Web 管理页面或 CLI 界面中，相同源/目的安全区域间多条域间策略始终按从上至下的显示顺序依次进行匹配（与策略 ID 号无关）。

除了管理员配置的自定义域间策略外，H3C Comware V5 平台防火墙还需考虑默认域间策略：其他安全区域都可以与 Local 区域互相访问；Management 区域仅能与 Management 区域或 Local 区域互相访问；除 Management 区域和 Local 区域外，高优先级安全区域可以主动访问低优先级安全区域，反之低优先级安全区域不可以主动访问高优先级安全区域，相同优先级安全区域之间可以互相访问；同一个安全区域内可以互相访问。默认域间策略不显示在配置界面中，它的匹配顺序始终在用户配置的域间策略之后。

防火墙域间策略支持引用"内容过滤策略模板"以实现对 HTTP、SMTP、POP3、FTP、Telnet 等 5 种协议的数据报文按特征执行过滤功能。当防火墙域间策略引用该配置模板时，需检查这部分配置是否正确并符合客户预期。

若防火墙域间策略启用了 MAC 地址匹配功能，需检查源/目的 MAC 地址配置是否正确，是否能够匹配实际业务报文的源/目的 MAC 地址。

部分型号防火墙支持域间策略加速功能，若发现加速状态失效，应先停止加速后再重新使能加速（该源/目的安全区域间策略数大于 1K），或停止加速即可（该源/目的安全区域间策略数小于 1K）。

在 Web 页面中，当某条域间策略的"启用选项"列显示为绿色箭头向上，表示该条域间策略当前为已启用状态，反之为不生效状态。

命令：*rule x permit*

rule x deny

source-ip xxxx

destination-ip xxxx

service x

rule enable

例如：在 CLI 管理界面中，进入安全域间视图，检查域间策略配置情况。本例中，Untrust 区域至 Trust 区域共有两条策略，禁止除 HTTP(TCP80)协议外的所有其他访问通过。

```
[H3C] interzone source Untrust destination Trust
[H3C-interzone-Untrust-Trust]display this
#
interzone source Untrust destination Trust
rule 5 permit
  source-ip any_address
```

```
      destination-ip any_address
      service http
      rule enable
    rule 6 deny
      source-ip any_address
      destination-ip any_address
      service any_service
      rule enable
  #
```

在 Web 管理界面的“防火墙→安全策略→域间策略”页签中，检查域间策略的配置情况，如图 6-64 所示。

源域 查询 | 高级查询

□	源域	目的域	ID	源IP地址	目的IP地址	服务	时间段	过滤动作	内容过滤策略模板	描述	启用选项	日志功能	源MAC地址	目的MAC地址	匹配次数	操作
□	Untrust	Trust	5	any_address	any_address	http		Permit			禁止	使能			0	
□	Untrust	Trust	6	any_address	any_address	any_service		Deny			禁止	使能			0	

新建 删除选中 导入 导出 清空统计

图 6-64 域间策略配置

命令：*display interzone-policy accelerate*

例如：通过命令查看域间策略加速状态是否正常，若状态列显示为“OOD”，说明当前加速状态已失效，应停止加速后再次重新使能加速功能。

```
<H3C> display interzone-policy accelerate
 S(Status): UTD -- up to date,   OOD -- out of date
 A(Accelerate): ACC -- accelerated,   UNACC -- unaccelerated

 Source-Zone              Destination-Zone                    A      S
 ----------------------------------------------------------------------
 Untrust                  Trust                               ACC    OOD
```

在 Web 管理界面的“防火墙→安全策略→策略加速”页签中，检查域间策略的加速状态，如图 6-65 所示。在本例中，Untrust 区域至 Trust 区域的策略加速状态为“失效”，必须手工操作重新加速，或停止加速。

ACL加速状态图标描述：●已加速 ○未加速 ●失效

源域	目的域	规则数量	ACL加速管理
Untrust	Trust	2	●加速

图 6-65 域间策略加速状态

(10) 检查地址对象配置

检查地址对象配置是否准确。对于主机地址和范围地址应重点检查有效 IP 地址、例外 IP 地址配置是否正确，以主机名方式配置的地址对象还需保证防火墙 DNS 解析功能正常，确保防火墙能够成功为主机名对象解析其对应的 IP 地址；对于子网地址对象，要特别注意其配

置为反掩码方式。对于地址组对象，要重点检查其引用的地址对象层次化关系是否准确。

命令：*object network subnet xxxx*

object network range xxxx

object network host xxxx

object-group network xxxx

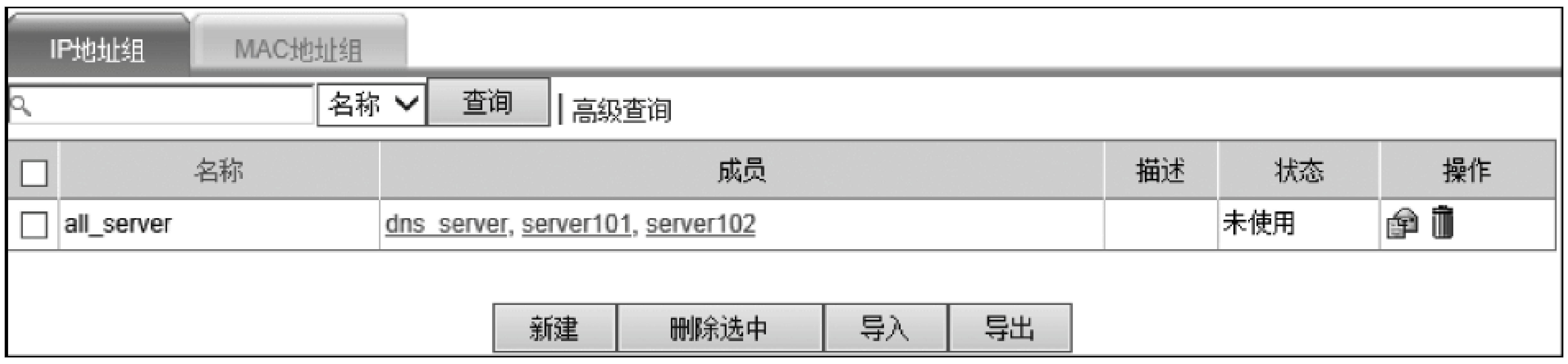
例如：在 CLI 管理界面中检查地址对象、对象组配置。

```
<H3C> display current-configuration | begin object
object network subnet 10.0.0.0/0.0.255.255
  subnet 10.0.0.0 0.0.255.255
 object network subnet 172.16.0.0/0.15.255.255
  subnet 172.16.0.0 0.15.255.255
 object network range dns_server
  range 192.168.255.30 192.168.255.40
  range exclude 192.168.255.33
 object network host server101
  host address 192.168.0.101
 object network host server102
  host address 192.168.0.102
 object-group network all_server
 object-group network all_server
  network-object dns_server
  network-object server101
  network-object server102
```

在 Web 管理界面的“资源管理→地址→IP 地址”页签中，可以查看到“主机地址”“范围地址”“子网地址”的配置情况，如图 6-66 所示，在“资源管理→地址→地址组”页签中，可以查看到“IP 地址组”的配置情况，如图 6-67 所示。



图 6-66　“主机地址”“范围地址”“子网地址”配置



IP地址组　MAC地址组

名称　查询　|高级查询

名称	成员	描述	状态	操作
all_server	dns_server, server101, server102		未使用	

新建　删除选中　导入　导出

图 6-67　“IP 地址组”配置

(11) 检查服务对象配置

检查服务对象配置是否准确。“预定义服务”是防火墙软件系统默认支持的常见协议、应用所对应的服务对象,支持通过命令查看,但不支持修改与删除。“自定义服务”是管理员根据实际组网应用情况创建的服务对象,需重点检查协议、端口号配置是否正确。在 Web 管理页面中任意端口号应表达为“0～65535”。对于服务组要确认其引用的服务对象层次化关系是否准确。

命令: *object service xxxx*

object-group service xxxx

例如: 在 CLI 管理界面中检查服务对象、服务对象组配置。

```
<H3C> display current-configuration | begin object
 object service http_8080
  service tcp destination-port 8080
 object service http_8081
  service tcp destination-port 8081
 object-group service all_http
  service-object http
  service-object http_8080
  service-object http_8081
```

在 Web 管理界面的“资源管理→服务→自定义服务”页签中,可以查看到“自定义服务”的配置情况,如图 6-68 所示,在“资源管理→服务→服务组”页签中,可以查看到“服务组”的配置情况,如图 6-69 所示。



名称　查询　|高级查询

名称	协议	协议参数	描述	状态	操作
http_8080	TCP	源端口:any, 目的端口:8080		未使用	
http_8081	TCP	源端口:any, 目的端口:8081		未使用	

新建　删除选中　导入　导出

图 6-68　“自定义服务”配置



名称　查询　|高级查询

名称	成员	描述	状态	操作
all_http	http, http_8080, http_8081		未使用	

新建　删除选中　导入　导出

图 6-69　“服务组”配置

(12) 检查时间段配置

查看防火墙当前系统时间、时区配置是否正确。若不正确应立即调整，建议启用 NTP 服务为防火墙实时同步系统时钟。注意不要同时启用 NTP 和 ACSEI 协议为防火墙插卡同步系统时间。

若系统时间正常，需检查时间对象配置是否正确。注意，当一个时间段配置中包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。如果当前系统时间正处于该时间对象生效的时间范围内，在用户界面上将有“Active”提示信息。

命令：*display clock*

例如：检查当前系统时间是否正常。

```
<H3C> display clock
16:14:57 Beijing Fri 07/08/2013
Time Zone :Beijing add 08:00:00
```

若系统时间不正确应立即调整。

命令：*clock datetime*

例如：通过命令调整系统时间。

```
<H3C> clock datetime 10:12 2013/05/03
```

命令：*time-range xxxx*

例如：在 CLI 管理界面中检查时间对象配置。

```
<H3C> display current-configuration | begin time-range
time-range working_time 08:30 to 18:00 working-day
```

命令：display *time-range xxxx*

例如：在 CLI 管理界面中检查时间对象当前是否生效。

```
<H3C> display time-range working_time
Current time is 16:14:57 7/8/2013 Monday

Time-range : working_time ( Active )
 08:30 to 18:00 working-day
```

在 Web 管理界面的“资源管理→时间段”页签中，可以查看到“时间段”的配置情况及生效状态，如图 6-70 所示。

名称	时间段描述	操作
working_time	(Active) 08:30 to 18:00 working-day	🗑

新建

图 6-70 “时间段”配置

(13) 是否启用双机热备

防火墙设备通常部署在网络中的重要节点位置，如果仅部署单台设备，当出现硬件故障时

将会对业务造成重大影响。因此在网络规划时，通常以两台防火墙硬件设备形成双机部署，从而避免出现单点故障，实现高可靠性。为真正实现快速热备份，需要在两台防火墙之间实时同步会话表项等信息，因此当两台防火墙形成双机关系，并且在网络中提供完全相同的功能时，应该启用防火墙双机热备功能。

命令：*display dhbk status*

例如：在 CLI 管理界面中检查是否启用双机热备，两台防火墙需分别进行检查。

```
<H3C> display dhbk status
 Stateful failover: Enabled
 Backup type: Symmetric path
 Current state: Synchronized
 Current port:
     GigabitEthernet0/4
 VLAN ID: 4094
```

在 Web 管理界面的“高可靠性→双机热备”页签中，可以查看是否启用双机热备，如图 6-71 所示。



图 6-71　双机热备配置

(14) 检查双机热备配置与状态

H3C Comware V5 平台防火墙双机热备功能分为会话同步、配置同步、IPSec SA 同步等几部分功能，其中会话同步又分为“不支持非对称路径”和“支持非对称路径”两种。

如果两台防火墙形成双机热备组网，双向业务流量仅经过主用防火墙转发，另一台备用防火墙正常情况下无业务流量，那么使能“不支持非对称路径”类型的双机热备会话同步即可；如果无法保证双向业务流量始终经过同一台防火墙转发，则必须使能“支持非对称路径”类型的双机热备会话同步。建议在两台防火墙之间，单独使用 1～2 条直联物理线路作为备份线。两台防火墙部署双机热备会话同步功能后，必须从组网规划上避免同一条业务流在源和目的之间转发时，同时经过两台防火墙；换言之，两台防火墙之间不应部署可以转发业务报文的二三层业务连接。

命令：*session synchronization enable*

　　　dhbk enable backup-type symmetric-path

dhbk enable backup-type dissymmetric-path

dhbk interface x vlan xxxx

display dhbk status

例如：在 CLI 管理界面中使能会话同步，启用防火墙双机热备支持非对称路径功能，选择 GE0/4＋VLAN4094 做双机热备口。备份线缆连接后，查看双机热备状态以确认配置生效。

```
[H3C] session synchronization enable
[H3C] dhbk enable backup-type dissymmetric-path
[H3C] dhbk interface GigabitEthernet0/4 vlan 4094
<H3C> display dhbk status
 Stateful failover: Enabled
 Backup type: Asymmetric path
 Current state: Synchronized
 Current port:
    GigabitEthernet0/4
 VLAN ID: 4094
```

在 Web 管理界面的“高可靠性→双机热备”页签中，也可进行双机热备会话同步的相关配置，如图 6-72 所示。注意，未使能配置同步功能时，配置同步状态将固定显示为“配置冲突”。



图 6-72　双机热备会话同步配置

如果两台防火墙形成双机热备组网，需要同步防火墙域间策略配置，可以在已经启用“使能双机热备功能”的前提下，通过启用配置同步功能实现。配置同步功能须在“配置主”设备，即管理员直接进行 Web 操作的这台防火墙上使能，另一台设备将自动成为“配置备”设备。功能启用后，设备管理员只需在“配置主”防火墙的 Web 页面上进行对象、域间策略及其他支持同步功能的配置增删、修改操作，另一台防火墙会自动同步“配置主”防火墙的对应配置。对于接口 IP 地址、VRRP、路由协议等功能，配置同步不会将“配置主”的配置同步给“配置备”设备，以避免出现配置错误。因此，在初始部署两台防火墙时，如果客户需要进行配置同步，强烈建议在防火墙尚处于出厂默认配置的状态下，优先开启双机热备配置同步功能，然后先在“配置主”设备上完成全部配置，再到“配置备”设备上补全不支持同步功能的配置，这样可以有效避免两台防火墙出现配置冲突。具体的配置操作方法可查询产品用户手册。

命令：*dhbk configuration-backup master synchronization*

例如：在 CLI 管理界面中使能配置同步功能。

```
[H3C] dhbk configuration-backup master synchronization
```

在 Web 管理界面的“高可靠性→双机热备”页签中，也可以启用双机热备配置同步功能。注意，在“配置主”设备上启用“使能双机热备功能”和“作为配置同步的主设备”，在“配置备”设备上启用“使能双机热备功能”即可。系统会自动选中两台防火墙的“自动同步更新配置”复选框。配置完成后，正常情况下同步状态将显示为“自动同步更新配置”。

如图 6-73 所示，成功使能双机热备配置同步的“配置主”防火墙状态。

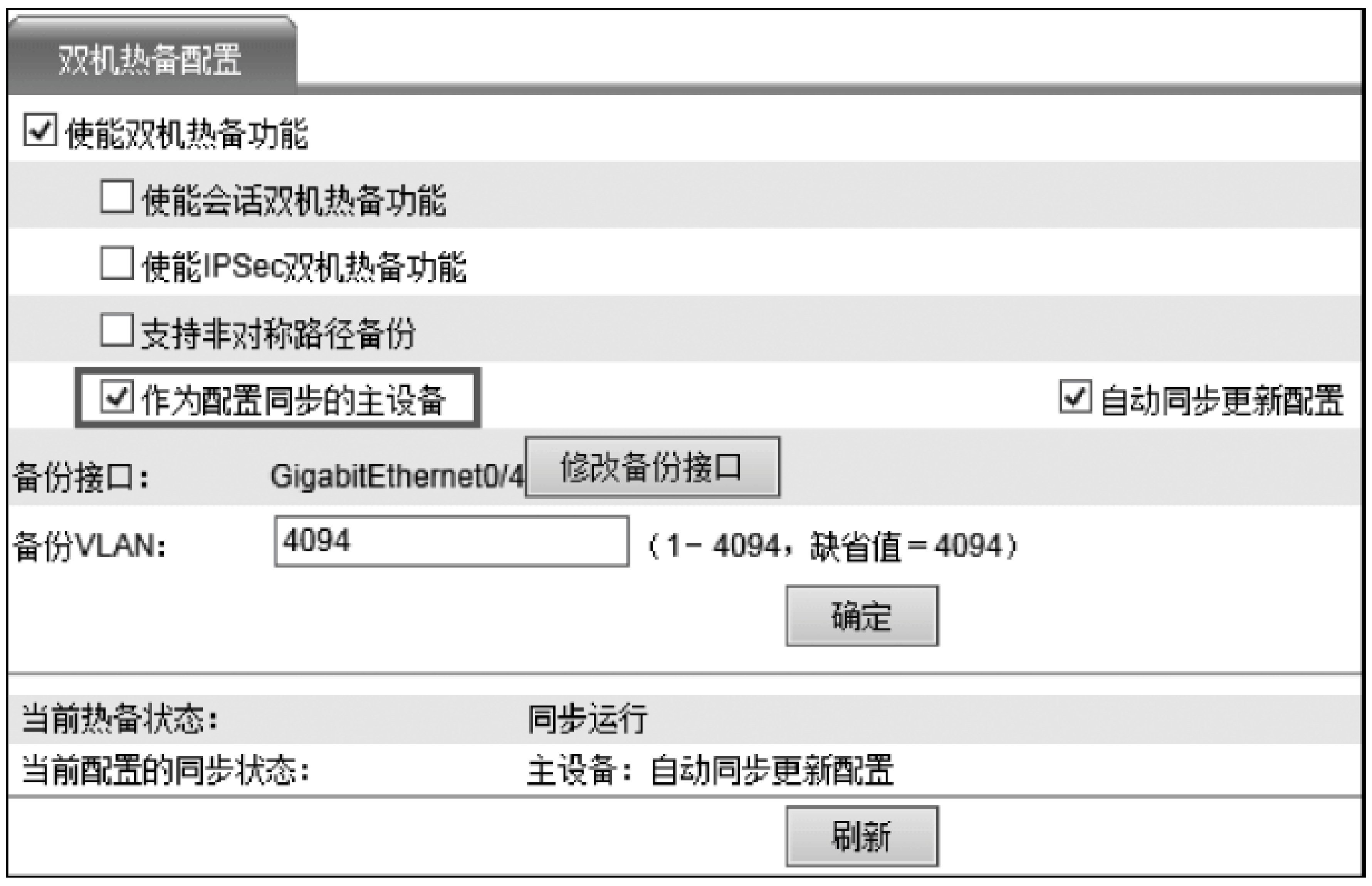


图 6-73 “配置主”防火墙

如图 6-74 所示，成功使能双机热备配置同步的“配置备”防火墙状态。

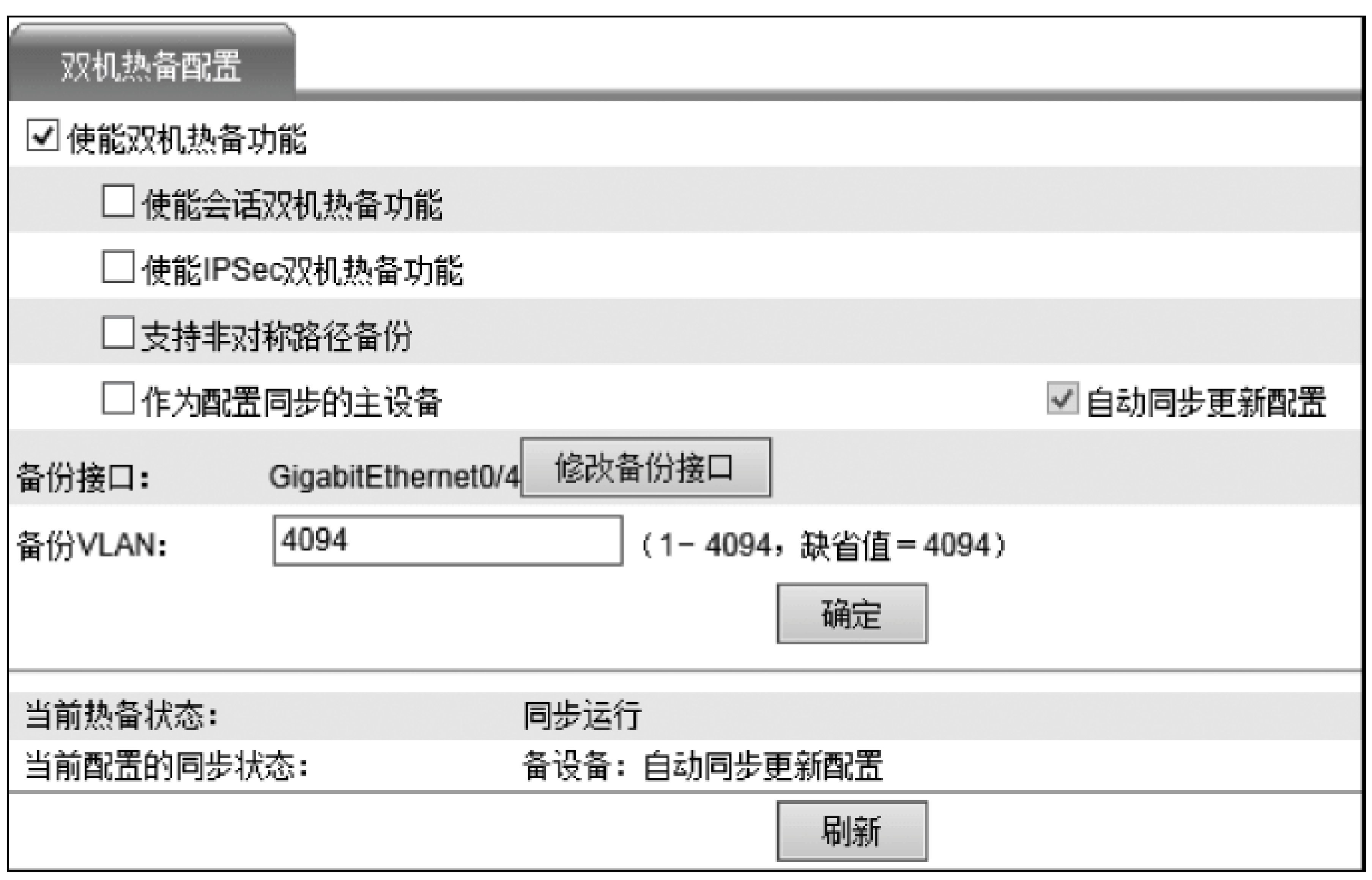


图 6-74 “配置备”防火墙状态


防火墙重启故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
煎 饼
开始
检查是否热重启
检查是否手工重启
检查设备供电
收集设备信息
拨打热线
400-810-0504
寻求帮助

1. 开始

防火墙重启问题定位故障的思路是：首先排除由于设备供电失败造成重启的可能，然后检查是否人为操作因素造成重启，确定是由于设备自身原因发生重启的，应尽快收集相关信息并反馈至 H3C 技术支持中心分析处理。

2. 流程图相关操作说明

(1) 检查是否热重启

查看设备最近一次重启类型。如果是热重启，则有可能是由于人为操作因素或设备自身因素引起；如果是冷重启，通常是由于供电不稳定、临时断电等原因引起。

命令：*display reboot-type*

例如：通过命令查看当前设备的最近一次重启类型。“Warm”表示热重启，“Cold”表示冷重启。

```
<H3C> display reboot-type
The rebooting type this time is: Warm

<H3C> display reboot-type
The rebooting type this time is: Cold
```

设备发生重启事件后，在 SNMP Trap 信息中也可以查看到对应的告警记录。

命令：*display trapbuffer reverse*

例如：通过命令查看当前设备 Trap 信息中有关重启的记录。同理，“Warm”表示热重启，“Cold”表示冷重启。

```
<H3C> display trapbuffer reverse
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages :2

#Dec  615:42:06:128 2013 H3C DEVM/4/SYSTEM WARM START:
 Trap 1.3.6.1.4.1.25506.6.8.5<hh3cSysWarmStartTrap>: system warm start.
...
#Dec  9 16:36:49:740 2013 H3C DEVM/4/SYSTEM COLD START:
 Trap 1.3.6.1.4.1.25506.6.8.4<hh3cSysColdStartTrap>: system cold start.
...
```

(2) 检查设备供电

设备发生冷重启常见于供电不稳定或临时中断后重新恢复的情形，也可能是设备管理员手工关闭电源开关或断开电源线强行使设备下电后重新恢复的情形，对于防火墙插卡则有可能是由于宿主路由交换主机下电、防火墙插卡被拔插等。在排查时，应当注意核实机房供电设施运行情况、UPS 电源工作情况等，对电源线、电源插排等也要仔细检查，避免接触不良或线

路问题。对于防火墙插卡，应当关注宿主路由交换主机是否存在电源故障、整机重启、防火墙板卡拔插动作等，可以通过路由交换主机的日志告警信息进行确认。

（3）检查是否手工重启

设备管理员手工重启防火墙可能的方式包括通过命令行、Web 配置页面直接操作防火墙重启，还包括网络管理员通过 SNMP 网管远程操作防火墙重启，以及通过宿主路由交换主机 OAP 命令间接重启防火墙插卡等。由于防火墙重启时其内存中的日志信息无法保存，因此必须借助日志主机、网管系统等协助确认。

（4）收集设备信息

如果已经确认防火墙在供电正常且无人为操作的前提下，出现无故重启现象，应尽快收集防火墙诊断信息、堆栈信息并反馈。如果防火墙出现罕见的反复重启现象，还需要将防火墙在反复重启过程中命令行界面所打印出的全部信息记录并反馈。

命令：*display diagnostic-information*

display exception 10 verbose

display exception 10 verbose from-device

例如：通过命令收集防火墙诊断信息、堆栈信息。收集诊断信息时，推荐采用先保存为文件，然后再下载并反馈的方式，如下所示。

```
<H3C> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]: y
Please input the file name( * .diag)[cfa0:/default.diag]:
Diagnostic information is outputting to cfa0:/default.diag.
Please wait...
Save successfully.

[H3C-hidecmd] display exception 10 verbose
-------------------------------exception info (no:   0)-------------------------------
Exception Number:                         0x20
Exception Name:                           NMI
Exception Instruction:                    0x80231EA8
Exception Slot:                           0
Exception VCpu:                           0
Exception Task:                           VIDL (TID: 3)
Exception Stack Base:                     0x82407fa8
Exception Time:                           2000-04-26   12:00:51
Exception Tick:                           0x0(CPU Tick High) 0xe2234e3c(CPU Tick Low)
...
```


防火墙链路聚合故障排查
翟运波
Hey THere
表示上一步结果正常
表示上一步结果出现问题
开始
查看成员端口选中状态
检查聚合口安全区域及域间策略
查看链路负载分担效果
检查成员端口配置
设置聚合组最大选中端口数
检查聚合组负载分担方式
查看成员端口是否超过聚合组上限
拨打热线
400-810-0504
寻求帮助

1. 开始

链路聚合通过将多条物理链路捆绑在一起成为一条逻辑链路，从而实现增加链路带宽和提高链路可靠性的目的，链路聚合定位问题的基本思路是：先查看成员端口选中状态、再查看端口流量负载分担情况，如果是防火墙等安全设备，还需要查看聚合口是否加入安全区域以及域间策略是否允许等信息。

2. 流程图相关操作说明

(1) 查看成员端口选中状态

聚合组内的成员端口有选中(Selected)和非选中(Unselected)两种状态，只有选中状态的成员端口才能够正常收发数据报文，所以首先要确保聚合组内的成员端口都处于选中状态。

命令：*display link-aggregation verbose* {*Bridge-Aggregation* / *Route-Aggregation*}

例如：通过命令查看聚合组 2 的成员端口 GE0/6 端口处于选中状态，GE0/7 处于非选中状态。

```
<H3C>display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation2
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 80f6-2ed3-9de8
Local:
  Port             Status  Priority  Oper-Key  Flag
--------------------------------------------------------------------------------
  GE0/6            S       32768     3         {ACDEF}
  GE0/7            U       32768     3         {AC}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE0/6            7       32768    1         0x8000, 0cda-4155-a9ee {ACDEF}
  GE0/7            8       32768    1         0x8000, 0cda-4155-a9ee {ACEF}
```

(2) 检查成员端口配置

要想让端口处于选中状态，首先必须保证端口的属性类配置(速率、双工和链路状态)和第二类配置(端口隔离、QinQ、VLAN 和 MAC 地址学习)和参考端口一致。如果是动态聚合，聚合口两端的聚合方式也要配置一致。

命令：*display interface xxx*

display current-configuration interface xxx

例如：通过命令查看接口速率、双工和 VLAN 配置正确。

```
<H3C>display interface GigabitEthernet 0/6
GigabitEthernet0/6 current state: Up
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0cda-4155-a9e7
 Description: GigabitEthernet0/6 Interface
 Loopback is not set
 Media type is twisted pair, loopback not set, promiscuous mode set

1000Mbps-speed mode, full-duplex mode
#
<H3C>display current-configuration interface GigabitEthernet 0/6
#
interface GigabitEthernet0/6
 port link-mode bridge
 port access vlan 20
 port link-aggregation group 2
#
[H3C]display current-configuration interface Bridge-Aggregation 2
#
interface Bridge-Aggregation2
 port access vlan 20
 link-aggregation mode dynamic
#
```

（3）查看成员端口是否超过聚合组上限

聚合链路的带宽取决于聚合组内选中端口的数量，在配置了聚合组中的最大选中端口数之后，聚合组内选中端口的最大数量将同时受配置值和端口硬件能力的限制，超过设备硬件能力或者配置的最大端口数以后，成员端口将不能被选中，只能作为备份接口。

命令：*display current-configuration interface xxx*

display link-aggregation verbose

例如：查看聚合组 Bridge-Aggregation 2 配置的成员端口数是三个，但配置允许的最大选中端口数为 2，所以实际选中的端口只有两个。

```
[H3C]display current-configuration interface Bridge-Aggregation 2
#
interface Bridge-Aggregation2
 port access vlan 20
 link-aggregation mode dynamic
link-aggregation selected-port maximum 2
#
[H3C]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:   A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
         D -- Synchronization, E -- Collecting, F -- Distributing,
         G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation2
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 0cda-4155-a9ee
```

```
Local:
  Port              Status  Priority  Oper-Key  Flag
--------------------------------------------------------------------------------
  GE0/6             S       32768     1         {ACDEF}
  GE0/7             S       32768     1         {ACDEF}
  GE0/8             U       32768     1         {ACD}
Remote:
  Actor             Partner Priority  Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE0/6             7       32768     3         0x8000, 80f6-2ed3-9de8 {ACDEF}
  GE0/7             8       32768     3         0x8000, 80f6-2ed3-9de8 {ACDEF}
  GE0/8             9       32768     3         0x8000, 80f6-2ed3-9de8 {AC}
```

(4) 设置聚合组最大选中端口数

默认情况下,设备不对聚合组中的最大选中端口数做限制,聚合组中的选中端口数仅受端口硬件能力的限制,可以通过命令设置每一个聚合组支持的最大选中端口数目。

命令:*link-aggregation selected-port maximum xxx*

例如:通过命令将聚合组 Bridge-Aggregation 2 的最大选中端口数设置成两个。

```
[H3C]interface Bridge-Aggregation 2
[H3C-Bridge-Aggregation2]display this
#
interface Bridge-Aggregation2
 port access vlan 20
 link-aggregation mode dynamic
 link-aggregation selected-port maximum 2
#
```

(5) 检查聚合口安全区域及域间策略

对于防火墙,必须将聚合接口加入安全区域才能转发数据,否则接口收到报文后全部丢弃。链路聚合后,只需要将聚合接口加入安全区域,不用再单独将每一个物理接口加入安全区域,如果设备做三层转发,需要同时将对应的 VLAN-Interface 接口也加入安全区域,最后再检查域间策略配置是否正确。

命令:*display current-configuration | begin zone*

例如:通过命令可以看到 Bridge-Aggregation1 和 VLAN-Interface10 加入 Trust 域,Bridge-Aggregation2 和 VLAN-Interface20 加入 Untrust 区域,Untrust 到 Trust 的域间策略也已经放开。

```
[H3C]display current-configuration | begin zone
zone name Trust id 2
 priority 85
 import interface Vlan-interface10
 import interface Bridge-Aggregation1 vlan 1 to 4094
zone name Untrust id 4
 priority 5
 import interface Vlan-interface20
 import interface Bridge-Aggregation2 vlan 1 to 4094
interzone source Untrust destination Trust
  rule 0 permit
```

```
source-ip any_address
destination-ip any_address
service any_service
rule enable
```

（6）查看链路负载分担效果

查看实际物理接口统计信息，看流量在聚合组的各成员端口上分发是否均匀。

命令：*display interface xxx*

例如：通过命令查看，可以看到聚合组 2 的成员端口 GE0/6 和 GE0/7 流量分担均匀。

```
[H3C]display interface GigabitEthernet 0/6
 GigabitEthernet0/6 current state: Up
1000Mbps-speed mode, full-duplex mode
Last 300 seconds input: 5 packets/sec 491 bytes/sec 0%
 Last 300 seconds output: 5 packets/sec 511 bytes/sec 0%
 Input (total): 10070 packets, 988552 bytes
          10002 unicasts, 0 broadcasts, 68 multicasts, 0 pauses
 Output (total): 10070 packets, 1028796 bytes
          10002 unicasts, 0 broadcasts, 68 multicasts, 0 pauses
...
[H3C]display interface GigabitEthernet 0/7
 GigabitEthernet0/7 current state: Up
1000Mbps-speed mode, full-duplex mode
Last 300 seconds input: 5 packets/sec 491 bytes/sec 0%
 Last 300 seconds output: 5 packets/sec 511 bytes/sec 0%
 Input (total): 10070 packets, 988680 bytes
 Output (total): 10070 packets, 1028960 bytes
          10000 unicasts, 0 broadcasts, 70 multicasts, 0 pauses
          10000 unicasts, 0 broadcasts, 70 multicasts, 0 pauses
...
```

（7）检查聚合组负载分担方式

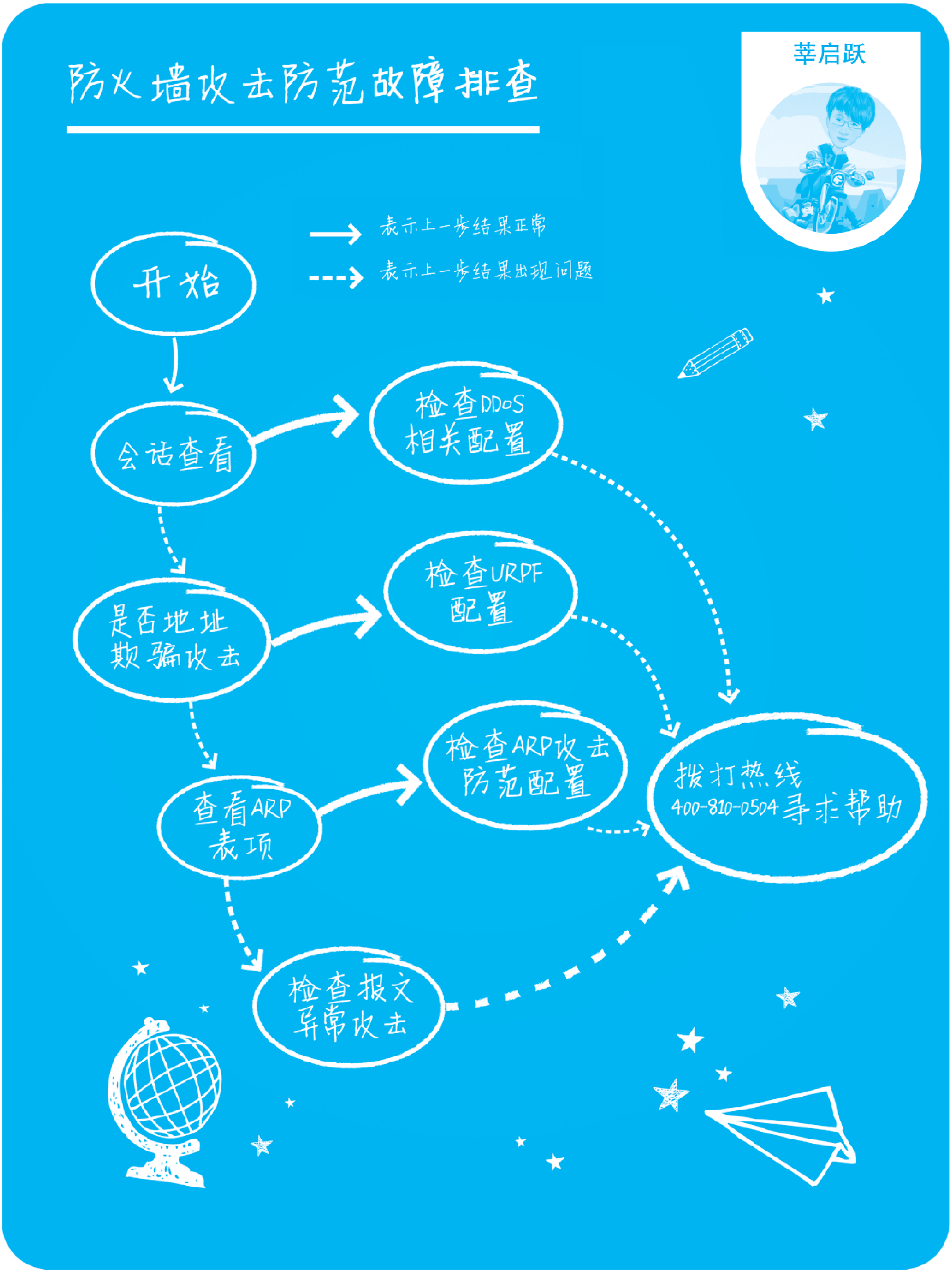
链路聚合可以根据报文的 MAC 地址、IP 地址、协议及端口信息进行哈希将流量分发到不同的物理链路，在实际组网中可以根据客户需求或者网络流量设置负载分担的方式。设备在全局或者链路聚合接口视图下设置负载分担方式，全局下设置对所有聚合组生效，接口下设置只对该聚合组生效，两者都设置的情况下，接口设置的分担方式优先。

命令：*link-aggregation load-sharing mode destination-ip source-ip ip-protocol*

display link-aggregation load-sharing mode interface interface-type interface-number

例如：通过命令查看并且设置链路聚合的负载分担方式。

```
[H3C] link-aggregation load-sharing mode destination-ip source-ip ip-protocol
[H3C]display link-aggregation load-sharing mode interface Bridge-Aggregation 1
Bridge-Aggregation1 Load-Sharing Mode:
  destination-ip address,  source-ip address,      ip-protocol
```



防火墙攻击防范故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
会话查看
检查DDoS相关配置
是否地址欺骗攻击
检查URPF配置
查看ARP表项
检查ARP攻击防范配置
检查报文异常攻击
拨打热线400-810-0504寻求帮助

1．开始

随着网络技术的普及,网络攻击行为出现得越来越频繁。各种网络病毒的泛滥,也加剧了网络被攻击的危险。

网络防火墙是一个或一组实施访问控制策略的系统,它监控可信任网络(相当于内部网络)和不可信任网络(相当于外部网络)之间的访问通道,以防止外部网络的危险蔓延到内部网络上。防火墙的攻击防范功能能够检测拒绝服务型、扫描窥探型、畸形报文型等多种类型的攻击,并对攻击采取合理的防范措施。攻击防范的具体功能包括黑名单过滤、报文攻击特征识别、流量异常检测和入侵检测统计。

排查故障的基本思路是:通过分析报文的内容特征和行为特征或者设备日志等信息判断开启的攻击类型是否正确,对攻击行为采取的措施检查是够满足当前情况。

2．流程图相关操作说明

有以下几种方式判断设备遇到哪种攻击。

(1) 会话查看

会话管理是为了实现NAT、ASPF、攻击防范等基于会话进行处理的业务而抽象出来的公共功能。此功能把传输层报文之间的交互关系抽象为会话,并根据发起方或响应方的报文信息对会话进行状态更新和超时老化。通过查看会话统计,来判断防火墙是否收到大量异常报文。

命令:*display session statistics*

例如:

① 出口遭到攻击,通过Wireshark抓到不正常的报文,这种大量源目地址固定,端口号不断变化的UDP报文,是端口扫描攻击,如图6-75所示。

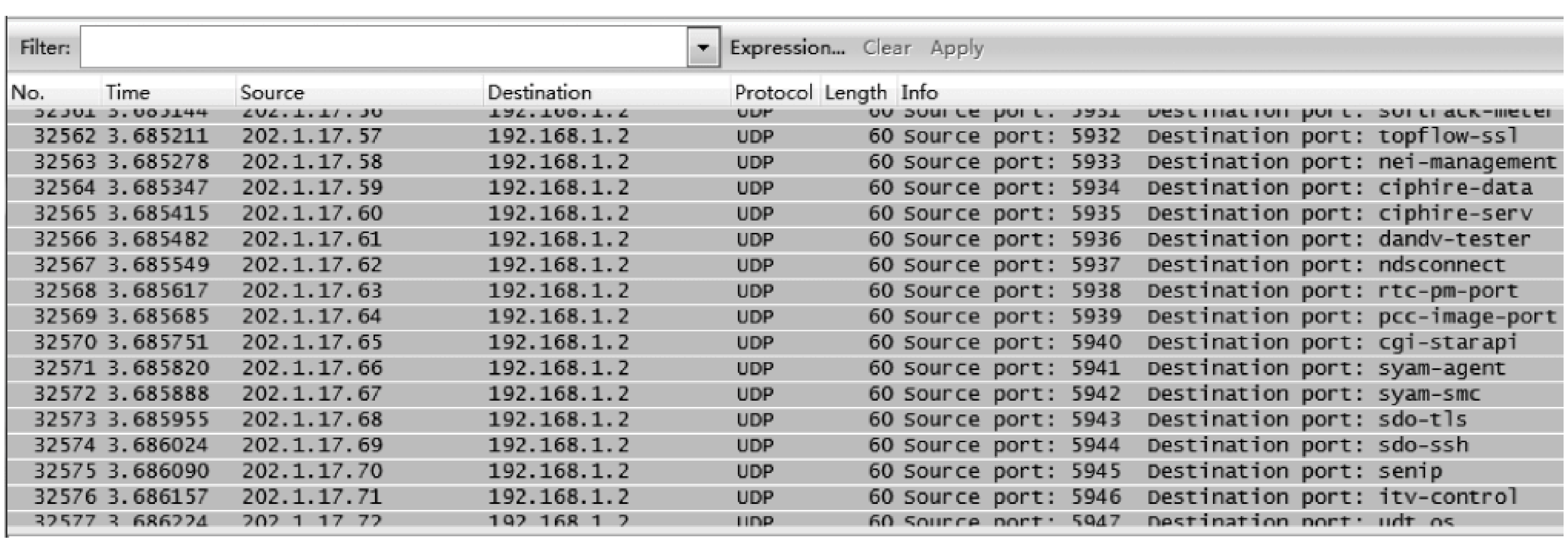


图6-75　端口扫描攻击

② 查看系统攻击日志或入侵检测统计,直接发现设备遇到哪种攻击。如图6-76所示,设备遇到ICMP Flood攻击。

安全区域：Trust

攻击类型	攻击次数	丢包个数
Fraggle	0	0
ICMP Redirect	0	0
ICMP Unreachable	0	0
Land	0	0
Large ICMP	0	0
Route Record	0	0
Scan	0	0
Source Route	0	0
Smurf	0	0
TCP Flag	0	0
Tracert	0	0
WinNuke	0	0
SYN Flood	0	0
ICMP Flood	0	0
UDP Flood	0	0
DNS Flood	0	0
基于源IP的连接数超出阈值	0	0
基于目的IP的连接数超出阈值	0	0

图 6-76 ICMP Flood 攻击

③ 查看会话统计。TCP、UDP、TCP 半连接数一目了然。如果 TCP 半连接数过多，有可能遇到 TCP 半连接攻击，如图 6-77 所示。

```
<H3C>display session statistics
Current session(s):2
        Current     TCP session(s): 2
                Half-Open: 0            Half-Close: 0
        Current     UDP session(s): 0
        Current    ICMP session(s): 0
        Current   RAWIP session(s): 0

Current relation table(s): 0

Session establishment rate:          0/s
        TCP     Session establishment rate:         0/s
        UDP     Session establishment rate:         0/s
        ICMP    Session establishment rate:         0/s
        RAWIP   Session establishment rate:         0/s

Received      TCP:              4604 packet(s)            1503295 byte(s)
Received      UDP:                 0 packet(s)                  0 byte(s)
Received     ICMP:                 0 packet(s)                  0 byte(s)
Received    RAWIP:                 0 packet(s)                  0 byte(s)
Dropped       TCP:                 0 packet(s)                  0 byte(s)
Dropped       UDP:                 0 packet(s)                  0 byte(s)
Dropped      ICMP:                 0 packet(s)                  0 byte(s)
Dropped     RAWIP:                 0 packet(s)                  0 byte(s)
```

图 6-77 TCP 半连接攻击

（2）是否 DDoS 流量攻击

拒绝服务型(Deny of Service，DoS)攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者主机挂起不能提供正常的工作。主要 DoS 攻击有 SYN Flood、Fraggle 等。拒绝服务攻击和其他类型的攻击不大一样，攻击者并不是去寻找进入内部网络的入口，而是去阻止合法的用户访问资源或路由器。

命令：*display session statistics*

例如：抓包如图 6-78 所示，把 TCP SYN 包的源地址和目标地址都设置成某一个受害者的 IP 地址。这将导致受害者向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。这是 Land 攻击，DoS 攻击的一种。

此外，还有 Smurf 攻击，Fraggle 攻击，Syn Flood 攻击，ICMP Flood 攻击等。

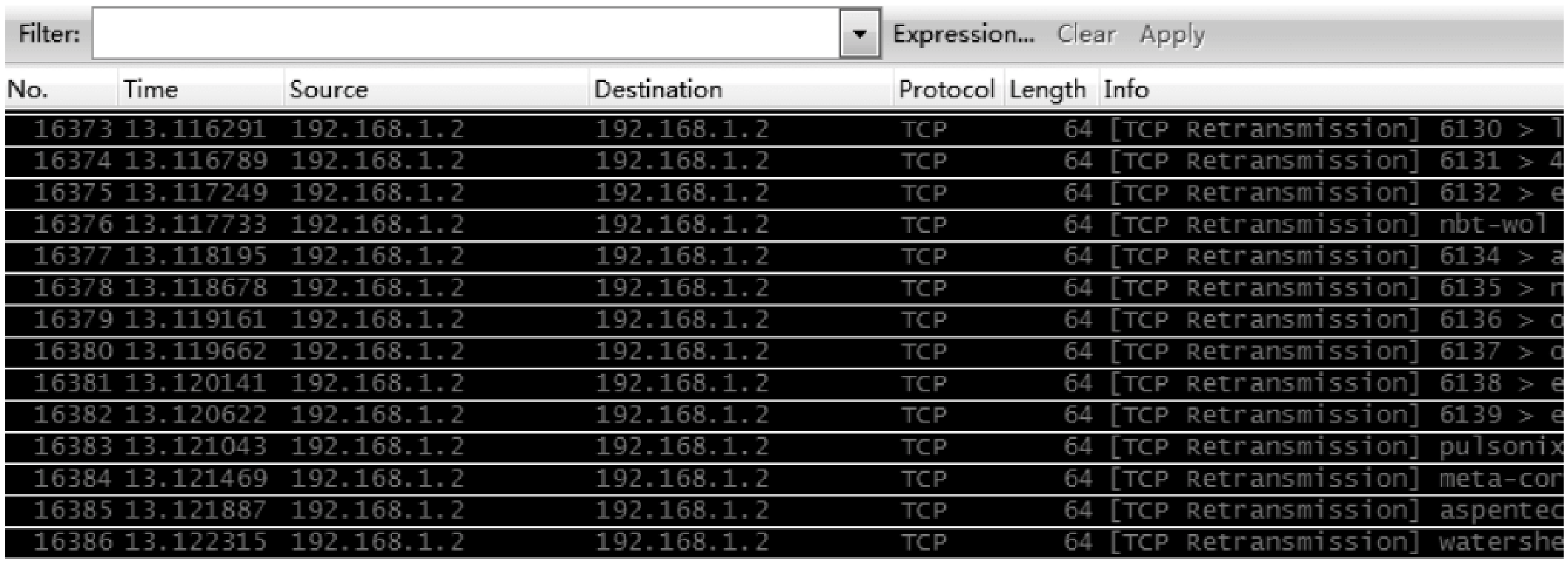


图 6-78　DDoS 流量攻击

通过命令 display session statistics 可以查看到骤然升高的异常连接数，以此做判断也可以。

(3) 检查 DDoS 相关配置

泛洪攻击检测主要用于保护服务器，通过监测向服务器发起连接请求的速率或者服务器上建立的半连接数量，来检测各类泛洪攻击，一般应用在设备连接内部网络的安全区域上，且仅对应用了攻击防范策略的安全区域的出方向报文有效。若设备检测结果显示向某服务器发起的连接请求的速率达到或超过了一定阈值，或服务器上建立的半连接数量达到或超过了一定数量(仅 SYN Flood 攻击检测支持半连接数限制)，则默认会输出告警日志，另外还可以根据配置对后续新建连接的报文进行丢弃处理。

流量异常检测。

例如：在 DMZ 域配置 SYN Flood 攻击检测，根据服务器的实际性能，配置服务器允许的最大新建连接速率为每秒 5000 个连接，当检测到攻击后阻断发往该服务器的后续连接。此需求需要在“攻击防范→流量异常检测→SYN Flood”路径下配置，如图 6-79 所示。

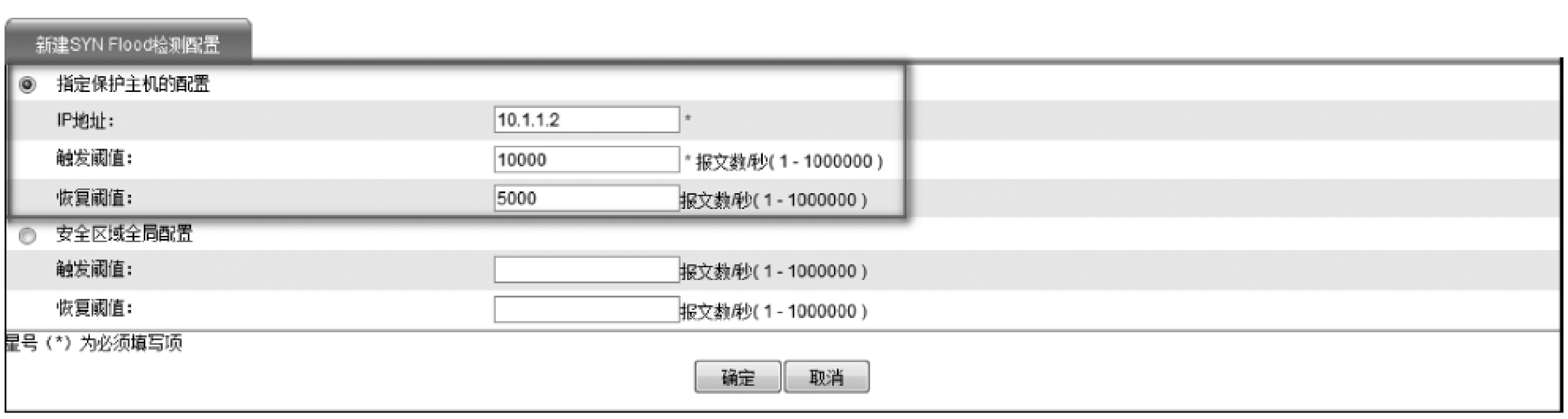


图 6-79　SYN Flood 检测配置

说明：Flood 攻击防范功能应在受保护区域开启。

设定触发阈值为 10000，表示每秒报文数达到 10000 后认为遇到攻击，并发出告警，如图 6-80 所示。

在全局下，可以选择“发现攻击丢弃报文”，但是有可能导致正常业务不通。另外，Syn Flood 攻击防范还可以使用 TCP Proxy 功能，如图 6-81 所示。

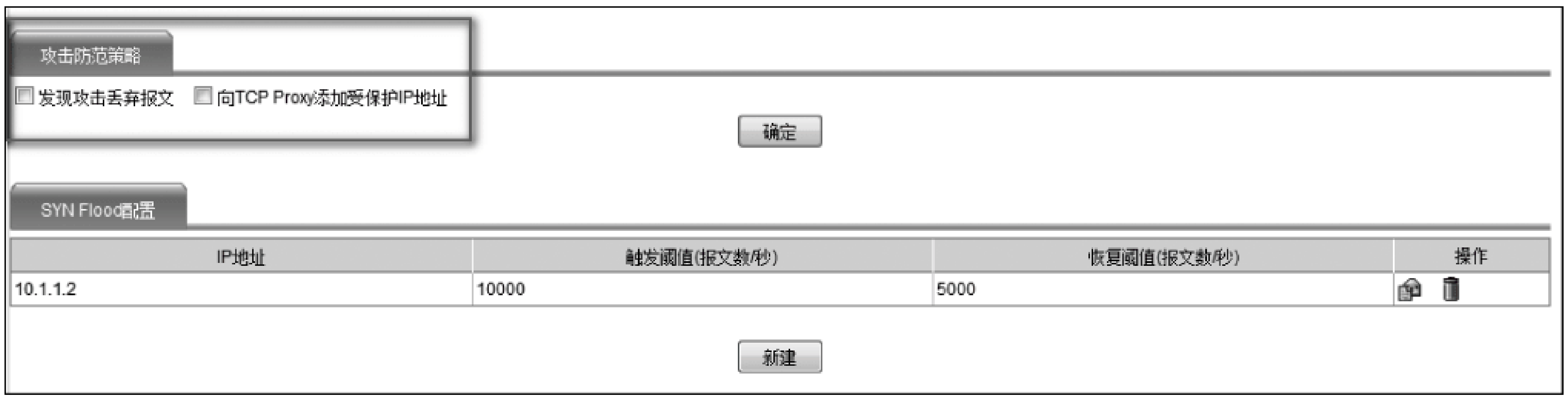


图 6-80　设定阈值



图 6-81　TCP Proxy 功能

TCP Proxy 功能用来防止服务器受到 SYN Flood 攻击。客户端通过 TCP 代理请求与受保护的服务器建立连接时，TCP 代理首先验证客户端的请求是否为 SYN Flood 攻击。验证通过后，客户端和服务器之间才能建立 TCP 连接，从而避免服务器受到攻击。

在“攻击防范→TCP Proxy→受保护 IP 配置”路径下可以手动添加被保护 IP，如果在 SYN Flood 攻击全局下选择“向 TCP Proxy 添加受保护 IP 地址”选项，则当被保护 IP 遇到攻击时动态添加进去。

然后开启双向的 trust 域内的代理功能，如图 6-82 所示。

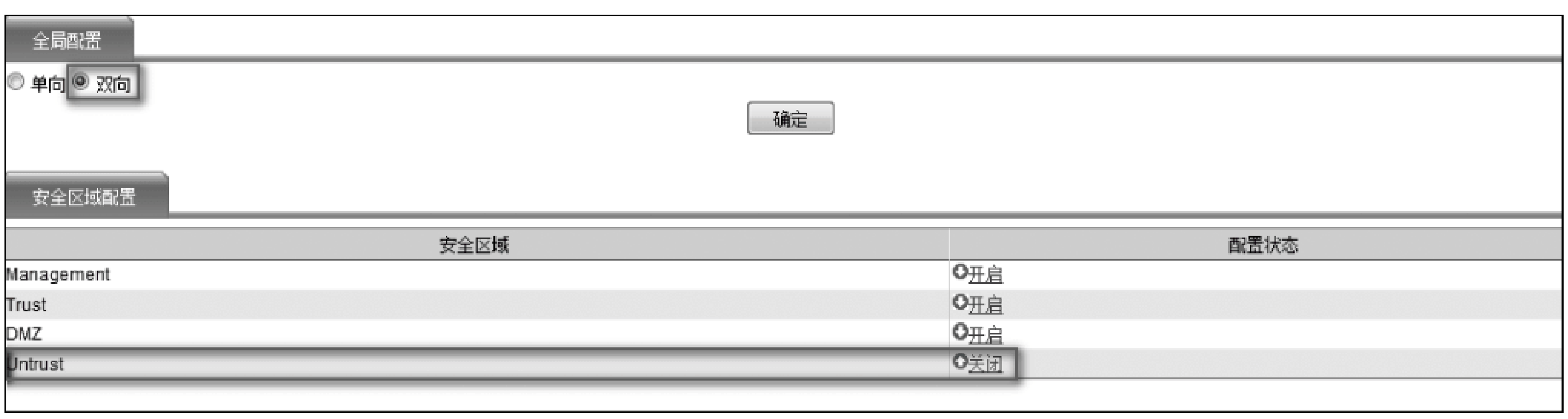


图 6-82　双向 trust 域内代理

单向代理方式是指仅对 TCP 连接的正向报文进行处理。双向代理方式是指对 TCP 连接的正向和反向报文都进行处理。被保护 IP 在哪个安全域就开启此安全域代理功能。

说明：TCP Proxy 功能只在安全区域的入方向生效。

(4) 是否地址欺骗攻击

地址欺骗攻击又称为 IP Spoofing 攻击。为了获得访问权，入侵者生成一个带有伪造源地址的报文。对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权的用户可以访问目的系统，甚至是以 root 权限来访问。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。这就造成 IP Spoofing 攻击，如图 6-83 所示。

例如：一般情况下，若从某接口不断发来源地址连续变化的报文，有可能是从一台主机发

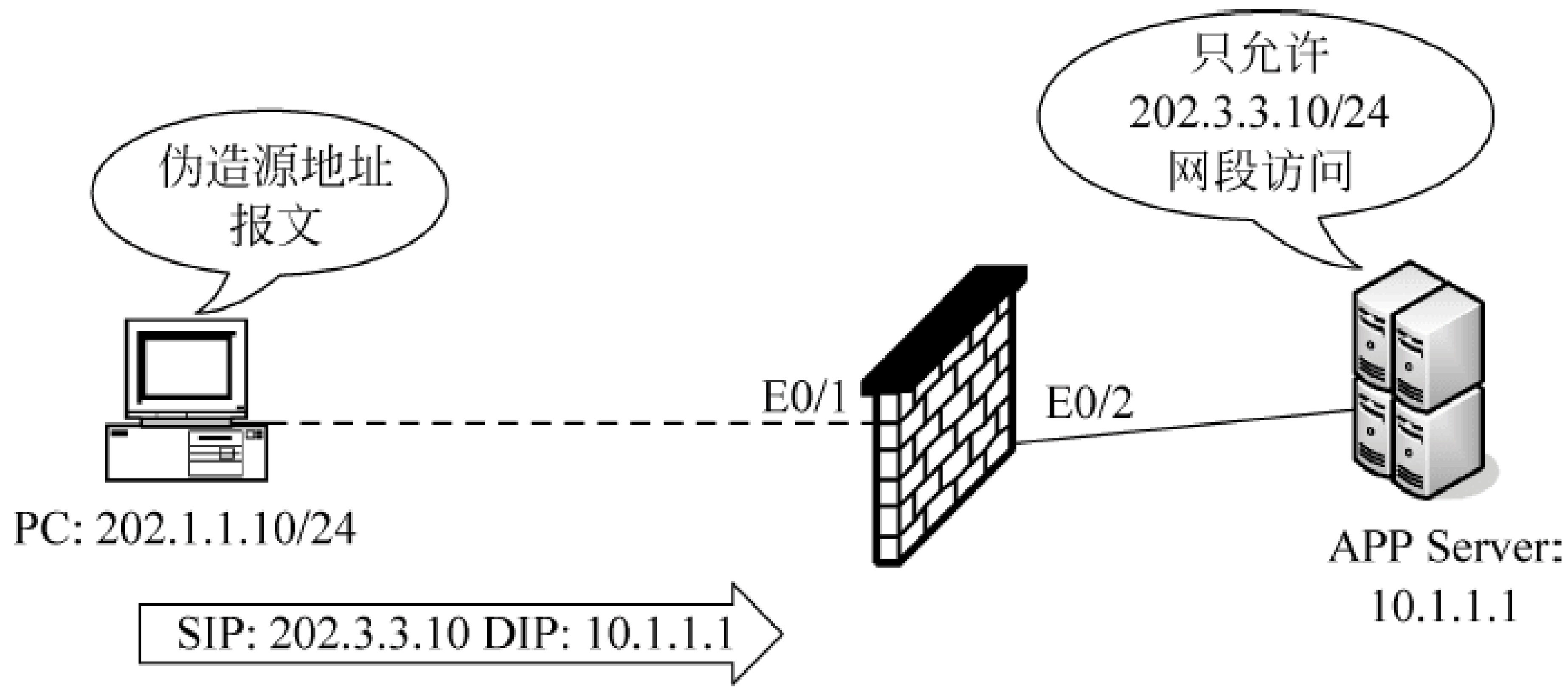


图 6-83　地址欺骗攻击原理

来，构造了虚假的源地址，如下面的日志所示。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]display  firewal session table verbose
 Total session number: 126730
  tcp, HTTP,
  58.68.95.205:27179-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:   timeout
  tcp, HTTP,
  58.68.194.45:47335-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:  00:00:04
  tcp, HTTP,
  58.68.148.155:55668-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:   timeout
  tcp, HTTP,
  58.68.194.44:47334-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:  00:00:04
  tcp, HTTP,
  58.68.148.154:55667-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:   timeout
  tcp, HTTP,
  58.68.27.45:39727-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:   timeout
  tcp, HTTP,
  58.68.107.15:25120-->61.147.103.125:80
  tag: 80000000,     ttl:  00:00:05     left:  00:00:03
  tcp, HTTP,
```

(5) 检查 URPF 配置

URPF(Unicast Reverse Path Forwarding，单播反向路径转发)的主要功能是用于防范基于源地址欺骗的网络攻击行为。

URPF 检测每个接口流入的 IP 报文的源地址与目的地址，并对报文的源地址反向查找路由表，入接口与以该 IP 地址为目的地址的最佳出接口不相同的 IP 报文被视为 IP Spoofing 攻击，将被拒绝，并进行日志记录。

URPF 检查有严格(Strict)型和松散(Loose)型两种。此外，还可以支持 ACL 与链路层、默认路由的检查。

URPF 的处理流程如下。

① 如果报文的源地址在设备的 FIB 表中存在。对于 Strict 型检查，反向查找报文出接口，若其中至少有一个出接口和报文的入接口相匹配，则报文通过检查；否则报文将被拒绝。

对于 Loose 型检查，报文通过检查。

② 如果报文的源地址在设备的 FIB 表中不存在，则检查默认路由及 URPF 是否配置了允许对默认路由进行处理。

对于没有配置允许对默认路由进行处理的情况，不管是 Strict 型检查还是 Loose 型检查，

只要报文的源地址在设备的 FIB 表中不存在，该报文都将被拒绝。

对于配置了默认路由，同时又配置了允许对默认路由进行处理的情况，如果是 Strict 型检查，只要默认路由的出接口与报文的入接口一致，则报文将通过 URPF 的检查；如果默认路由的出接口和报文的入接口不一致，则报文将被拒绝。如果是 Loose 型检查，报文都将通过 URPF 的检查，进行正常的转发。

命令：无

举例：启动 URPF，要求严格检查，同时允许对默认路由进行特殊处理，如图 6-84 所示。

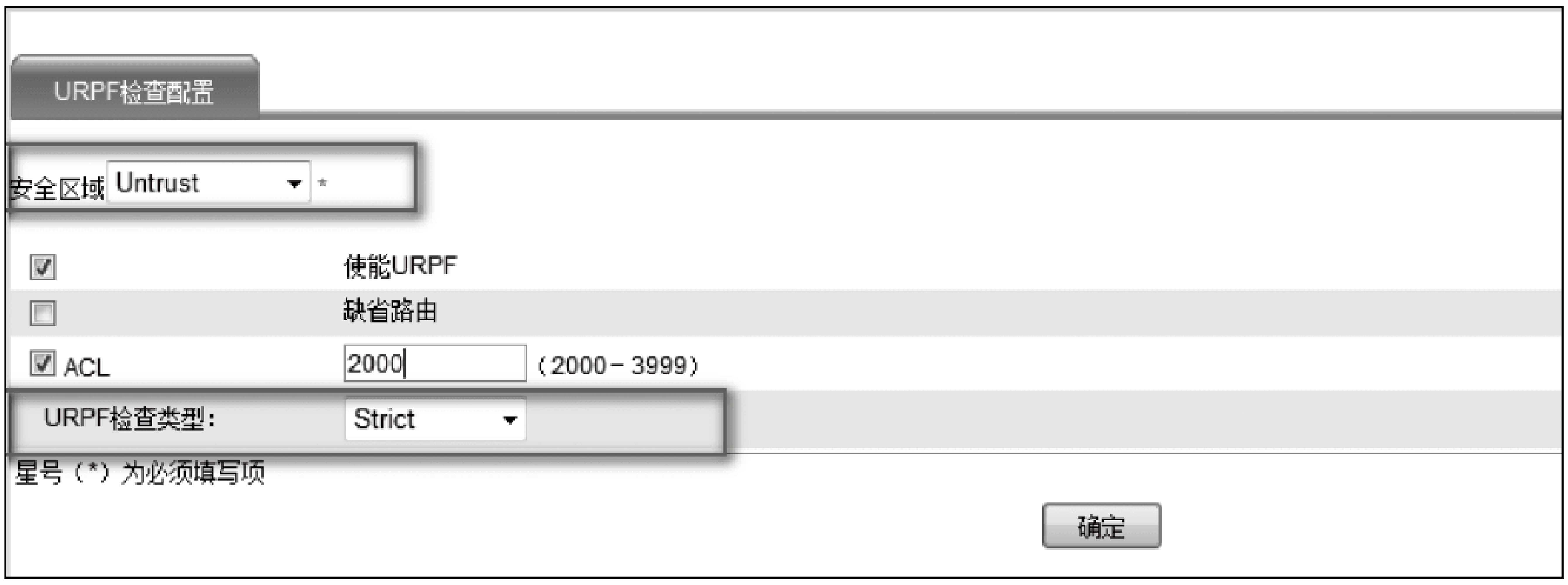


图 6-84　URPF 检查配置

说明： URPF 检查仅对安全区域中接口收到的报文有效。

对于广播地址，直接予以丢弃。

对于全零地址，如果目的地址不是广播，则丢弃。（源地址为 0.0.0.0，目的地址为 255.255.255.255 的报文，可能是 DHCP 或者 BOOTP 报文，不做丢弃处理。）

当且仅当报文被拒绝后，才去匹配 ACL。如果被 ACL 允许通过，则报文继续进行正常的转发（此类报文称为被抑制丢弃的报文）；如果被 ACL 拒绝，则报文被丢弃。

其他选项请参照上文或配置手册。

（6）是否 ARP 攻击

以太网网络中的主机，在互相进行 IP 访问之前，都必须先通过 ARP 协议来获取到目的 IP 地址对应的 MAC 地址。在通过路由器、三层交换机作为网关时，主机为了把数据发送到网关，同样需要通过 ARP 协议来获取网关的 MAC 地址。由于 ARP 协议本身不具备任何的安全性，所以留下了很多的安全漏洞。

对于 ARP 攻击，可以抓包看是否收到大量 ARP 报文，或者查看 ARP 表项检查 MAC 地址与 IP 地址映射是否有变化。

命令：*dis arp all/dynamic*

例如：查看 ARP 映射表项，如图 6-85 所示。

（7）检查 ARP 攻击防范配置

ARP 攻击有以下防范方式。

① 定时发送免费 ARP 功能可以及时通知下行设备更新 ARP 表项或者 MAC 地址表项。

② ARP 自动扫描与固化。

举例如下。

```
<H3C>dis arp all
                 Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface              Aging Type
10.255.255.25    3ce5-a612-2ae6  N/A      GE0/1                  7     D
10.255.255.24    3ce5-a613-ff07  N/A      GE0/1                  7     D
10.255.255.23    0023-8934-4a82  N/A      GE0/1                  8     D
10.255.255.12    3ce5-a613-3f39  N/A      GE0/1                  20    D
10.255.255.11    3ce5-a681-f111  N/A      GE0/1                  20    D
10.255.255.101   3ce5-a682-c521  N/A      GE0/1                  10    D
10.255.255.22    000f-e2e0-44e8  N/A      GE0/1                  19    D
10.255.255.14    3ce5-a613-fe58  N/A      GE0/1                  17    D
10.255.255.21    000f-e287-3c2a  N/A      GE0/1                  5     D
10.255.255.102   3ce5-a682-c5bc  N/A      GE0/1                  13    D
10.255.255.1     000f-e2ec-2da2  N/A      GE0/1                  6     D
10.255.255.91    0023-89a6-893b  N/A      GE0/1                  6     D
10.255.255.15    3ce5-a612-2a29  N/A      GE0/1                  6     D
10.255.255.92    3ce5-a615-7246  N/A      GE0/1                  6     D
10.255.255.43    c4ca-d9dc-f26f  N/A      GE0/1                  6     D
10.255.255.33    c4ca-d9dc-f288  N/A      GE0/1                  6     D
10.255.255.62    80f6-2ec3-ae01  N/A      GE0/1                  6     D
10.255.255.44    c4ca-d9dc-f274  N/A      GE0/1                  6     D
10.255.255.34    c4ca-d9dc-f26a  N/A      GE0/1                  6     D
10.255.255.61    80f6-2ec3-c001  N/A      GE0/1                  7     D
```

图 6-85　ARP 映射表项

① 免费 ARP。设置定时发送免费 ARP 报文的接口和发送间隔时间，如图 6-86 所示。



图 6-86　设定时间

说明：配置本功能后，只有当接口链路 Up 并且配置 IP 地址后，此功能才真正生效；如果修改了免费 ARP 报文的发送周期，则在下一个发送周期才能生效。

② ARP 自动扫描功能一般与 ARP 固化功能配合使用。如图 6-87 所示，启用 ARP 自动扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。



图 6-87　启用 ARP 自动扫描

说明：如果不指定 ARP 自动扫描区间，则仅对接口下的主 IP 地址网段内的邻居进行扫描。其中，发送的 ARP 请求报文的源 IP 地址就是接口的主 IP 地址；开始 IP 地址和结束 IP 地址必须与接口的 IP 地址（主 IP 地址或手工配置的从 IP 地址）在同一网段。

如图 6-88 所示，ARP 固化功能用来将当前的 ARP 动态表项（包括 ARP 自动扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效地防止攻击

者修改 ARP 表项。

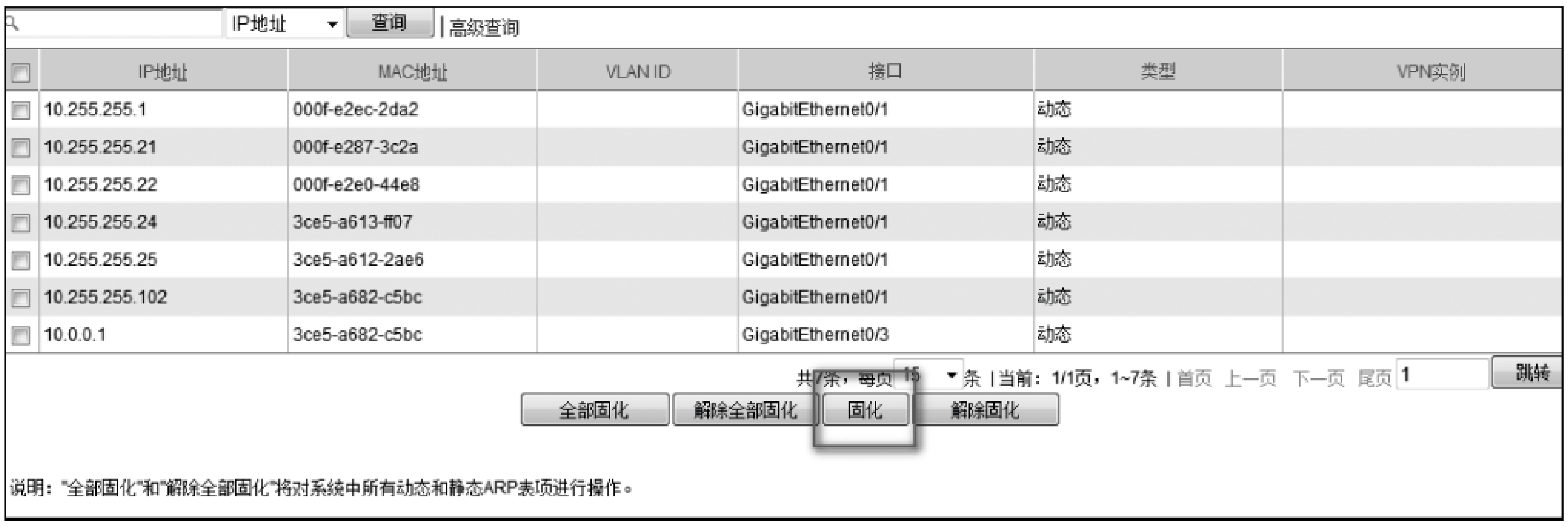


图 6-88　ARP 固化

例如：出接口运营商网关 MAC 地址是固定，一般不会时常变化，而出接口又容易受到攻击，所以为了防止 ARP 攻击，可以启用固化。

（8）异常报文攻击

单包攻击也称为畸形报文攻击。攻击者通过向目标系统发送有缺陷的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩溃，给目标系统带来损失，或者通过发送大量无用报文占用网络带宽等行为来造成攻击。

常见特殊报文攻击有以下几种：Fraggle，Land，WinNuke，TCP Flag，ICMP Unreachable，ICMP Redirect，Tracert，Smurf，Source Route，Large ICMP，Route Record 等。

（9）选择安全域并选中相应防范功能

报文异常检测功能可以通过分析经过设备的报文特征来判断报文是否具有攻击性，一般应用在设备连接外部网络的安全区域上，且仅对启用了报文异常检测功能的安全区域的入方向报文有效。若设备检测到某报文具有攻击性，则默认会输出告警日志，另外还可以根据配置将检测到的攻击报文做丢弃处理。

说明：*报文异常检测需在攻击源所在安全域开启。*

例如：防范外部网络 Untrust 对内部网络 trust 主机的 Land 攻击和 Smurf 攻击，发现攻击丢包，如图 6-89 所示。

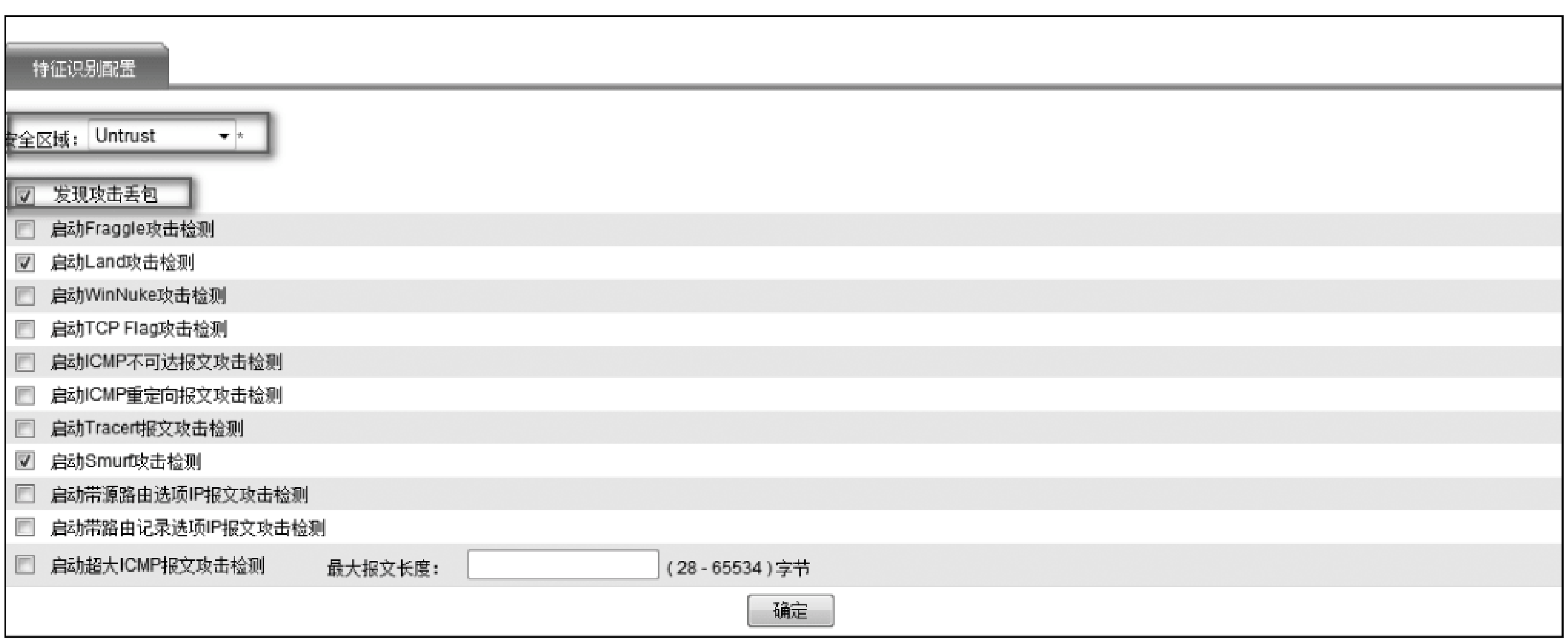


图 6-89　发现攻击丢包

防火墙ALG故障排查

酉海华



→ 表示上一步结果正常

- - -> 表示上一步结果出现问题



1. 开始

ALG 技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。本文通过查看防火墙相关配置，排查 ALG 功能使用的正确性。

2. 流程图相关操作说明

(1) 查看相关 ALG 功能是否开启

新版本的防火墙默认关闭了大部分 ALG 功能，只开启了最常用的 FTP。在后续的配置中，可以根据需求选择某一项进行开启

命令：*display this*

例如：查看当前 alg 开启状态，只会显示未开启的 ALG 功能。

```
[H3C]dis this
…
undo alg dns
 undo alg rtsp
 undo alg h323
 undo alg sip
 undo alg sqlnet
 undo alg pptp
 undo alg ils
 undo alg nbt
 undo alg msn
 undo alg qq
 undo alg tftp
 undo alg sccp
 undo alg gtp
```

(2) 查看会话状态

确认相关 ALG 功能开启后，查看当前会话的状态，并查看是否成功建立关联表项。

命令：*display session table source-ip x.x.x.x verbose*

display session statistics

例如：通过命令查看，可以确认会话正常。

```
[H3C]display session table source-ip 192.168.1.1 ver
Initiator:
  Source IP/Port : 192.168.1.1/5000
  Dest IP/Port   : 183.60.16.208/8000
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 183.60.16.208/8000
  Dest IP/Port   : 60.191.99.139/1199
  VPN-Instance/VLAN ID/VLL ID:
Pro: UDP(17)      App: QQ             State: UDP-READY
Start time: 2013-07-02 21:28:57   TTL: 9s
```

```
Root                          Zone(in): Trust
                              Zone(out): Untrust
Received packet(s)(Init): 1 packet(s) 111 byte(s)
Received packet(s)(Reply): 1 packet(s) 71 byte(s)
[H3C]dis session statistics
Current session(s):5
        Current      TCP session(s): 4
                  Half-Open: 0               Half-Close: 2
        Current      UDP session(s): 1
        Current     ICMP session(s): 0
        Current    RAWIP session(s): 0

Current relation table(s): 1

Session establishment rate:          0/s
        TCP      Session establishment rate:        0/s
        UDP      Session establishment rate:        0/s
        ICMP     Session establishment rate:        0/s
        RAWIP    Session establishment rate:        0/s

Received      TCP:        1563 packet(s)       206376 byte(s)
Received      UDP:         491 packet(s)        46888 byte(s)
Received     ICMP:          45 packet(s)         3548 byte(s)
Received    RAWIP:           0 packet(s)            0 byte(s)
Dropped       TCP:           0 packet(s)            0 byte(s)
Dropped       UDP:           0 packet(s)            0 byte(s)
Dropped      ICMP:           0 packet(s)            0 byte(s)
Dropped     RAWIP:           0 packet(s)            0 byte(s)
```

(3) 查看会话关联表项

查看防火墙设备上生成的关联表项。

命令：*display session relation-table*

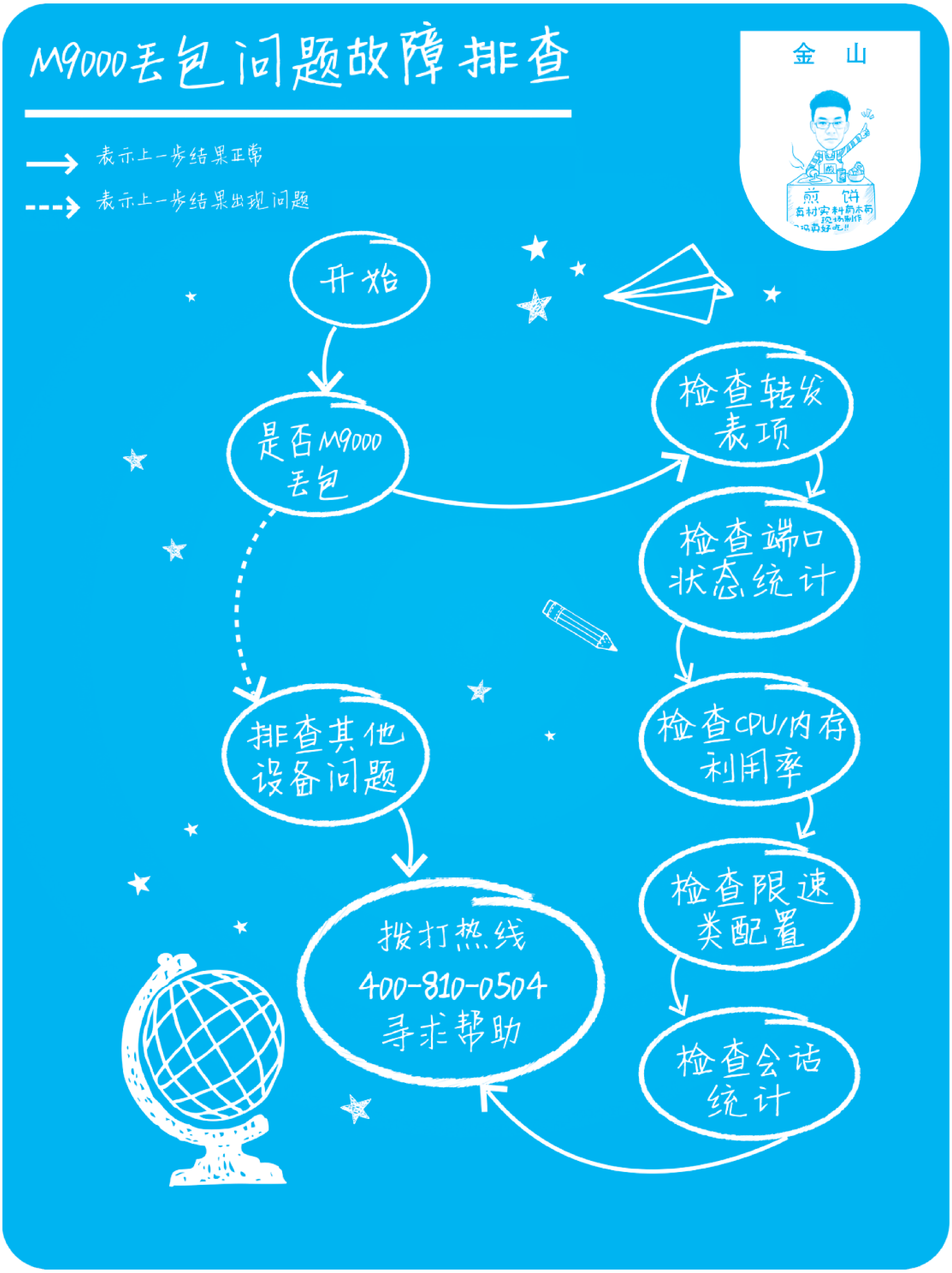
例如：通过命令查看，可以确认生成了相应的关联表项。

```
[H3C]dis session relation-table
Local IP/Port              Global IP/Port           MatchMode
192.168.1.1/51234          60.191.99.139/1224       Either
 App: unknown          Pro: UDP     TTL: ---     AllowConn 4294967295
 Total find: 1
```

如果确认上述均正常，收集诊断信息。

命令：*display diagnostic-information*

收集完成以后通过 FTP 下载文件。


M9000丢包问题故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
煎 饼
开始
是否M9000丢包
检查转发表项
检查端口状态统计
检查CPU/内存利用率
检查限速类配置
检查会话统计
排查其他设备问题
拨打热线
400-810-0504
寻求帮助

1. 开始

M9000 丢包问题定位故障的思路是：首先确定发生丢包的具体位置和方向，然后再具体分析产生丢包的原因。须注意：本云图中的 M9000 丢包问题，主要指客户业务的双方向数据报文经设备转发后，出现部分报文被丢弃而未能转发至目标设备的问题，即并不是完全不通类问题。M9000 设备的业务端口板支持硬件流量统计特性，因此可以利用流量统计策略确认丢包发生的准确位置及方向，以便判断问题是否由 M9000 造成；然后再依次对 M9000 的转发表项、端口状态、CPU/MEM、限速相关配置等进行检查；如果问题现象为偶发的临时性丢包，则应重点检查当丢包发生时的会话表项统计数据、端口统计数据、CPU/MEM 统计数据等。如果会话统计值出现异常（每秒新建会话速率/并发连接数远超日常数据），通常是由于突发性异常流量短时内在 M9000 上创建大量会话表项，进而影响了设备转发性能导致。这类故障一般通过合理优化配置或直接消除异常流量攻击来源即可解决。

2. 流程图相关操作说明

（1）是否 M9000 丢包

丢包类问题常常于现场工程师利用 ICMP ping 测试发现。因此可以通过对 ping 测试的数据包实施流量统计，以进一步明确丢包问题是否发生在本 M9000 设备上。这种利用 ICMP 报文丢弃情况来考察实际业务报文丢弃情况的方法，在多数场景中都是极具参考意义的。流量统计策略即流行为是“accounting”的 QoS 策略，可以下发在 M9000 与上下行设备互联的业务端口上。如果无法实施流量统计策略，也可以通过在流量入/出 M9000 的端口位置进行镜像抓包，通过对比进入设备之前和经过设备之后的报文情况来判断数据包经转发后，是否出现了丢包、乱序等异常现象。

命令：*acl number xxxx*

rule x permit icmp source x.x.x.x 0 destination x.x.x.x 0

traffic classifier xxxx

if-match acl xxxx

traffic behavior xxxx

accounting

qos policy xxxx

classifier xxxx behavior xxxx

qos apply policy xxxx inbound enhancement

qos apply policy xxxx outbound enhancement

displayqos policy interface xxxx

例如：通过在 M9000 与上下行设备互联端口双方向配置流量统计策略，可以观察 10.0.0.1（客户端_Ten-GE1/0/1）与 172.16.0.1（服务器_Ten-GE1/0/2）之间的 ping 报文在经过 M9000 转发时，是否存在丢包。具体配置方法为先创建两条 ACL，分别匹配正反方向的 ICMP 报文，然后配置流量统计策略，应用在内联口上。注意，要对上行/理行方向经过 M9000 入/出的报文分别进行统计，这样不仅可以判断防火墙是否有丢包，还可以同时判断在哪个方

向上存在丢包。注意,ACL 规则的配置必须精确,否则会使统计策略匹配无关报文,影响统计结果和问题判断。

```
#
[H3C] acl number 3001
[H3C-acl-adv-3001] rule 5 permit icmp source 10.0.0.1 0 destination 172.16.0.1 0
#
[H3C] acl number 3002
[H3C-acl-adv-3002] rule 5 permit icmp source 172.16.0.1 0 destination 10.0.0.1 0
#
[H3C] traffic classifier client_to_server
[H3C-classifier-client_to_server] if-match acl 3001
#
[H3C] traffic classifier server_to_client
[H3C-classifier-server_to_client] if-match acl 3002
#
[H3C] traffic behavior acc
[H3C -behavior-acc] accounting
#
[H3C] qos policy c_to_s
[H3C-qospolicy- c_to_s] classifier client_to_server behavior acc
#
[H3C] qos policy s_to_c
[H3C-qospolicy-s_to_c] classifier server_to_client behavior acc
#
[H3C-Ten-GigabitEthernet1/0/1] qos apply policy c_to_s inbound enhancement
[H3C-Ten-GigabitEthernet1/0/1] qos apply policy s_to_c outbound enhancement
[H3C-Ten-GigabitEthernet1/0/2] qos apply policy s_to_c inbound enhancement
[H3C-Ten-GigabitEthernet1/0/2] qos apply policy c_to_s outbound enhancement
```

流量统计策略配置完成后,进行 ping 测试,然后查看统计结果。通过对比双向的报文收发统计,就可以查看总共发送至 M9000 多少个报文,从 M9000 转发多少个报文。如果从 M9000 接收的报文个数大于同方向转发的报文个数,则说明本设备确实出现丢包情况。如果 M9000 本身未丢包,同方向接收报文数与发送报文数相等,但 ping 发起方至 ping 响应方统计到的报文个数少于 ping 操作的报文次数,则可以判断丢包是出现在 ping 发起方与 M9000 之间的某个位置;反之,若 ping 发起方至 ping 响应方统计到的报文个数等于 ping 操作的报文次数,但大于 ping 响应方至 ping 发起方统计到的报文个数,则说明丢包是出现在 ping 响应方与 M9000 之间的某个位置。

如示例所示,从客户端向服务器端总共 ping 10 次,ping 测试结果显示通了 9 次,1 次超时。流量统计策略结果显示,正方向 10 个报文全部到达了 M9000 并且转发了 10 个报文;而反方向仅从连接服务器的端口接收到 9 个报文并转发。该结果证明,网络中确实存在丢包问题,但不是 M9000 引入的;同时,可以判断丢包是发生在服务器与 M9000 之间的某个位置上。

```
<H3C> display qos policy interface Ten-GigabitEthernet 1/0/1
  Interface: Ten-GigabitEthernet1/0/1

  Direction: Inbound

  Policy:c_to_s
   Classifier: client_to_server
```

```
            Operator: AND
            Rule(s) : If-match acl 3001
            Behavior: accounting
             Accounting Enable:
               10 (Packets)

        Direction: Outbound

        Policy:s_to_c
         Classifier: server_to_client
            Operator: AND
            Rule(s) : If-match acl 3002
            Behavior: accounting
             Accounting Enable:
               9 (Packets)

     <H3C> display qos policy interface Ten-GigabitEthernet 5/0/1
        Interface: Ten-GigabitEthernet5/0/1

        Direction: Inbound

        Policy:s_to_c
         Classifier: server_to_client
            Operator: AND
            Rule(s) : If-match acl 3002
            Behavior: accounting
             Accounting Enable:
               9 (Packets)

        Direction: Outbound

        Policy:c_to_s
         Classifier: client_to_server
            Operator: AND
            Rule(s) : If-match acl 3001
            Behavior: accounting
             Accounting Enable:
               10 (Packets)
```

(2) 排查其他设备问题

若确认丢包问题不是由 M9000 引起,应进一步排查其他设备问题。判断丢包发生的具体位置及方向仍可参考步骤(1)中提供的思路及方法。当网络中存在其他支持流量统计策略的设备时,建议可采用分段排查法,逐步缩小范围。如果最终定位丢包确由非 H3C 品牌设备引起,建议及时联系相应的技术服务团队分析处理。

(3) 检查转发表项

排查 M9000 转发丢包问题,首先要检查相关的 ARP/路由等转发表项是否正确。在丢包现象出现时,应反复执行查看命令,以确认是否存在表项频繁振荡。针对转发表项错误的,应进一步对相应的功能模块进行检查,排除错误信息。针对转发表项频繁振荡的,可以先利用手工配置的静态表项暂时替代,然后再进一步查明振荡原因,消除其对转发的影响。

命令: *display arp*

display ip routing-table

例如：通过命令检查 M9000 设备学习的 ARP 表项及路由表项是否正确。

```
<H3C>display arp
   Type: S-Static    D-Dynamic    O-Openflow    R-Rule    I-Invalid
IP address     MAC address      VLAN      Interface            Aging Type
172.16.20.2    7425-8a76-d42a   N/A       RAGG2                17    D
172.16.10.1    0023-8938-2720   N/A       RAGG1                17    D
<H3C> display ip routing-table
Destinations : 26        Routes : 26

Destination/Mask    Proto      Pre  Cost       vNextHop        Interface
0.0.0.0/0           Static     60   0          172.31.0.1      MGE1/0/0/0
0.0.0.0/32          Direct     0    0          127.0.0.1       InLoop0
10.255.255.1/32     O_INTRA    10   5          172.16.10.1     RAGG1
10.255.255.2/32     Direct     0    0          127.0.0.1       InLoop0
10.255.255.3/32     O_INTRA    10   2          172.16.20.2     RAGG2
10.255.255.4/32     O_INTRA    10   7          172.16.20.2     RAGG2
```

（4）检查端口状态统计

检查 M9000 端口物理层、链路层状态是否正常，检查端口的速率、双工协商状态，注意同时检查对端接口的相关属性是否与本端协商一致。检查端口出方向队列是否发生拥塞、是否出现错包等。若端口状态异常或入方向错包统计持续增加，则应优先检查物理线路是否存在故障，建议通过替换法进行对比测试。如果物理端口采用的是光口，还需要检查光模块状态参数是否正常，是否与对端一致，同时注意检查光纤是否正常。

命令：*display interface interface-type interface-number*

例如：通过命令检查 M9000 端口 GigabitEthernet 1/0/1 的状态和统计信息。

```
<H3C> display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1 current state: Up
Line protocol current state: Up
Description: GigabitEthernet1/0/1 Interface
The Maximum Transmit Unit is 1500
Internet Address is 10.255.255.13/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e280-de8e
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e280-de8e
Media type is twisted pair, loopback not set, promiscuous mode not set
1000Mb/s, Full-duplex, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queuing : Size/Length/ Discards)  0/100/ 0
Output queue : (Protocol queuing : Size/Length/ Discards)  0/500/ 0
Output queue : (FIFO queuing : Size/Length/ Discards)  0/75/ 0
Last clearing of counters: Never
    Last 300 seconds input rate 43 bytes/sec, 344 bits/sec, 0 packets/sec
    Last 300 seconds output rate21 bytes/sec, 110 bits/sec, 0 packets/sec
    Input: 2375264 packets, 0 jumboes, 151311918 bytes, 2375264 buffers
           272229 broadcasts, 6757 multicasts, 0 pauses
           0 errors, 0 runts, 0 giants
           0 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
    Output:17451 packets, 7045543 bytes, 17451 buffers
           2 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 underruns, 0 collisions
           0 deferred, 0 drops, 0 lost carriers
```

(5) 检查 CPU/内存利用率

检查设备 CPU/内存利用率，确认设备是否出现业务繁忙。若 CPU/内存利用率持续保持在较高水平(超过 70%)，可参考 CPU/内存利用率高问题排查云图处理。通常情况下，与正常运行状态的设备相比 CPU/内存利用率持续较高，多由异常攻击流量造成，因此在排查时要关注设备当前所接收到的流量情况是否正常，是否存在并发连接数量大、每秒新建连接数量高的异常流量冲击。针对这种情况，比较有效的方法是通过抓包等手段先查看具体的异常流量，判断其来源，然后再通过黑名单、域间策略、攻击防范、路由交换设备上的包过滤策略等手段屏避该流量；如果异常流量来源自内网，建议直接找出并消除攻击源。对于其他非业务流量引起的 CPU/内存利用率高问题，情况复杂处理困难的，可以及时记录信息并反馈。

命令：*display cpu-usage*

display memory

例如：通过命令查看 M9000 的 CPU/内存利用率。要特别注意检查安全业务板的利用率是否过高。

```
<H3C>display cpu-usage
Chassis 1 Slot 1 CPU 0 CPU usage:
        2% in last 5 seconds
        2% in last 1 minute
        2% in last 5 minutes

Chassis 1 Slot 4 CPU 0 CPU usage:
        0% in last 5 seconds
        0% in last 1 minute
        0% in last 5 minutes

Chassis 1 Slot 7 CPU 0 CPU usage:
        1% in last 5 seconds
        1% in last 1 minute
        1% in last 5 minutes

Chassis 1 Slot 7 CPU 1 CPU usage:
        0% in last 5 seconds
        0% in last 1 minute
        0% in last 5 minutes

<H3C>display memory
The statistics about memory is measured in KB:
Chassis 1 Slot 1:
              Total    Used      Free    Shared    Buffers    Cached    FreeRatio
Mem:         984640  368180    616460         0          0     93436        62.6%
-/+ Buffers/Cache:     274744    709896
Swap:             0         0         0

Chassis 1 Slot 4:
              Total    Used      Free    Shared    Buffers    Cached    FreeRatio
Mem:        2245296  889112   1356184         0       1148    292984        60.4%
-/+ Buffers/Cache:     594980   1650316
Swap:             0         0         0
```

```
Chassis 1 Slot 7:
              Total    Used       Free    Shared    Buffers    Cached     FreeRatio
Mem:         984640  368776     615864         0          0     93436         62.5%
-/+ Buffers/Cache:       275340     709300
Swap:                0          0          0

Chassis 1 Slot 7 CPU 1:
              Total    Used       Free    Shared    Buffers    Cached     FreeRatio
Mem:       16375504 2459404   13916100         0       1368    148744         85.0%
-/+ Buffers/Cache:   2309292   14066212
Swap:                0          0          0
```

(6) 检查限速类配置

M9000 设备支持端口限速、流量监管、队列调度等 QoS 特性。当设备上启用含有限速特性的功能配置后，当业务流量超过了配置的限速值时，超出承诺信息速率的部分会被设备丢弃，所以应当检查业务流量大小是否超过了配置的限速值，QoS 策略统计是否有丢弃报文计数等。

命令：*display qos lr interface x*

display qos queue interface x

display qos car interface x

displayqos policy interface x

例如：在 CLI 界面下，查看端口限速统计情况。可以看到统计结果显示已有 10 个报文因 CAR 限速策略被丢弃。

```
<H3C>display qos car interface GigabitEthernet 1/1/0/23
Interface: GigabitEthernet1/1/0/23
 Direction: outbound
  Rule: If-match any
   CIR 8 (kbps), CBS 1875 (Bytes), EBS 0 (Bytes)
   Green action      : pass
   Yellow action     : pass
   Red action        : discard
   Green packets     : 14 (Packets), 20188 (Bytes)
   Yellow packets    : 0 (Packets), 0 (Bytes)
   Red packets: 10 (Packets), 14420 (Bytes)
```

(7) 检查会话统计

M9000 从业务端口接收到报文后，会利用会话表项对该报文是否符合协议状态机、是否为域间策略、ASPF 策略等进行一系列检查，对检查不通过的报文将丢弃处理。在正常运行过程中，M9000 会不断地新建会话表项和保持会话表项，如果在会话表项老化时间内，始终没有再接收到双向业务报文时还会主动删除该会话表项。在防火墙的会话表统计信息中，网络管理员可以查看到新建会话速率、当前并发会话总数、接收报文统计、丢弃报文统计等。通过将新建会话速率、并发会话总数与日常运维过程中所观察记录的数据做对比，可以大致判断设备运行状态是否正常，设备是否正在受到异常流量攻击并创建了大量的无效会话等。

命令：*display session statistics*

display session statistics summary

例如：某 M9000 在正常运行过程中，管理员通过命令观察到会话统计信息如下所示。

2 号框 7 号槽位防火墙业务板会话表项总数为 4.7 万，其中 TCP 会话 13529 个，会话表项新建速率为 6644/s，实际网络业务运行正常。

```
<H3C>display session statistics
CPU 1 on slot 7 in chassis 2:
Current sessions:47685
          TCP sessions:           13529
          UDP sessions:           32315
         ICMP sessions:            1799
       ICMPv6 sessions:               0
     UDP-Lite sessions:               0
         SCTP sessions:               0
         DCCP sessions:               0
        RAWIP sessions:              42

Current relation-table entries: 0

Session establishment rate:6644/s
          TCP:            1596/s
          UDP:            4889/s
         ICMP:             152/s
       ICMPv6:               0/s
     UDP-Lite:               0/s
         SCTP:               0/s
         DCCP:               0/s
        RAWIP:               7/s

Received TCP       :      74787448 packets          5687988432 bytes
Received UDP       :    3846597878 packets         14787444751 bytes
Received ICMP      :        327487 packets             4658432 bytes
Received ICMPv6    :             0 packets                   0 bytes
Received UDP-Lite  :             0 packets                   0 bytes
Received SCTP      :             0 packets                   0 bytes
Received DCCP      :             0 packets                   0 bytes
Received RAWIP     :         35878 packets              753052 bytes
```

在某时间点用户反馈网络突然出现丢包问题，通过命令观察到如下所示的会话统计信息。其中，会话总数已经激增到 2000 万，其中 TCP 会话超过 1900 万，TCP 协议新建会话速率达到 26 万，远远高于日常观察值。从以上信息可以初步判断，目前网络中 TCP 协议流量存在异常，可能存在 TCP SYN Flood 攻击类流量。针对这类攻击，可以先利用当前设备的会话表项详细信息来分析特点和来源，如果攻击是来源于网络外部或 Internet 的，一般通过启用攻击防范手段来防御，方法包括黑名单、域间策略、流量异常检测等；如果攻击是来源于网络内部的，最好的方法就是直接找到这个内部攻击源并消除。

```
<H3C>display session statistics
CPU 1 on slot 7 in chassis 2:
Current sessions:20000313
          TCP sessions:           19948812
          UDP sessions:              49865
         ICMP sessions:               1598
       ICMPv6 sessions:                  0
     UDP-Lite sessions:                  0
```

```
    SCTP sessions:              0
    DCCP sessions:              0
   RAWIP sessions:             38

Current relation-table entries: 0

Session establishment rate:266628/s
          TCP:          261503/s
          UDP:            5017/s
         ICMP:             108/s
       ICMPv6:               0/s
     UDP-Lite:               0/s
         SCTP:               0/s
         DCCP:               0/s
        RAWIP:               9/s

Received TCP       :       124787448 packets          8687988321 bytes
Received UDP       :      4346597228 packets         19787486751 bytes
Received ICMP      :          567417 packets             7358852 bytes
Received ICMPv6    :               0 packets                   0 bytes
Received UDP-Lite  :               0 packets                   0 bytes
Received SCTP      :               0 packets                   0 bytes
Received DCCP      :               0 packets                   0 bytes
Received RAWIP     :           65865 packets             1553078 bytes
```

M9000内存高问题故障排查



1. 开始

M9000 内存高问题故障排查的思路是：首先判断是否内存高，如果高的话找出具体哪些进程或者功能模块占用较多资源，并收集相关信息反馈分析。

2. 流程图相关操作说明

（1）判断内存情况

首先查看设备各槽位板卡内存使用情况，判断是否存在某板卡内存异常。内存达到 70% 以上需要引起注意。

① 分布式设备——独立运行模式/集中式 IRF 设备。

display memory [*slot slot-number* [*cpu cpu-number*]]

② 分布式设备——IRF 模式。

display memory [*chassis chassis-number slot slot-number* [*cpu cpu-number*]]

命令：*display memory*

举例：slot0 主控板的内存剩余仅 6.8%，已非正常情况。

```
<M9000>display memory
The statistics about memory is measured in KB:
Chassis 1 Slot 1:
           Total      Used      Free     Shared    Buffers    Cached     FreeRatio
Mem:      2752152    2565496   186656         0         68    248964        6.8%
-/+ Buffers/Cache:   23166464   435688
Swap:                   0          0          0
```

（2）检查重启类型

当发现内存正常时，有可能设备之前发生过因内存问题引起的重启。这样也是不正常的，可以通过命令查看。一旦发现内存问题重启，也需要反馈收集的内存信息、设备诊断和 logfile。

命令：*display version*

举例：通过 display version 命令来查看某个板卡是否发生重启，重启原因如果是内存问题会显示“Memory exhaust”。

```
<M9000>display version
H3CComware Software, Version 7.1.054, Release 9115P04
Copyright (c) 2004-2015 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
...
LPU Chassis 1 Slot 1:
Uptime is 2 weeks,1 day,18 hours,39 minutes
H3CSecPath M9010 LPU with 1 XLS408 Processor
BOARD TYPE:          NSQ1GP24TXEA0
DRAM:                1024M bytes
FLASH:               0M bytes
NVRAM:               0K bytes
PCB 1 Version:       VER.B
```

```
Bootrom Version:          511
CPLD 1 Version:           003
CPLD 2 Version:           002
Release Version:          H3CSecPath M9010-9115P04
PatchVersion    :         None
RebootCause     :         Memory exhaust
…
```

(3) 检查具体内存情况

① 想要知道板卡哪个进程或者模块占用较多内存,需要进一步收集内存态和用户态内存信息。

命令:*display system internal kernel memory pool chassis x* slot *x*(收集指定板卡的内核态内存池信息)

```
[M9000]probe
[M9000-probe]display system internal kernel memory pool chassis 1 slot 1
Active    Number  Size    Align  Slab  Pg/Slab  ASlabs  NSlabs  Name
2         19      768     0      19    4        1       1       sgpool-32
0         60      2048    0      15    8        0       4       mbuf_db
371       640     24      0      64    1        9       10      anon_vma
0         0       20      0      64    1        0       0       Lipc_QEntCache
0         0       88      4      32    1        0       0       cfq_queue
0         0       28      0      64    1        0       0       inotify_event_cache
…
```

命令:*display process memory*(收集用户态内存信息,每个槽位都是一样的)

```
[M9000]display process memory
   JID       Text      Data      Stack    Dynamic    Name
     1        132       696         32        152    scmd
     2          0         0          0          0    [kthreadd]
     3          0         0          0          0    [migration/0]
     4          0         0          0          0    [ksoftirqd/0]
     5          0         0          0          0    [watchdog/0]
…
```

命令:*display system internal kernel memory pool chassis x slot*

display process memory

举例:收集内核态内存占用情况,其中 kmalloc-128 占用了超过 1GB 内存(8907738 * 128=1087MB),如图 6-90 所示。

② 如果是内核态内存异常,则需查看某内存池的内存明细。

命令:*[M9000-probe]display system internal kernel memory pool name xxx*

举例:如图 6-91 所示,确认进程 0xf2f0000 消耗了大量内存。

(4) 检查重启类型

内存不正常时,也有可能设备之前发生过因内存问题引起的重启。可以通过命令查看。一旦发现内存问题重启,也需要反馈信息。内存信息、设备诊断和 logfile 一并收集。

命令:*display version*

```
[GDSZ-PS-ISG04-FW01-probe]dis system internal kernel memory pool chassis 1 slot 0
Active    Number  Size   Align Slab Pg/Slab ASlabs  NSlabs Name
7363      7560    2048   8     15   8       502     504    kmalloc-2048
1416      1792    512    8     28   4       62      64     kmalloc-512
8907344   8907738 128    8     42   2       212086  212089 kmalloc-128
3911      4326    32     8     42   1       103     103    kmalloc-32
2338      2816    8      8     64   1       43      44     kmalloc-8
1685      2058    96     8     42   2       49      49     kmalloc-96
7099      7488    168    0     36   2       200     208    vm_area_struct
0         0       24     0     51   1       0       0      fasync_cache
62        63      4096   8     7    8       9       9      kmalloc_dma-4096
0         28      4096   0     7    8       0       4      mbuf_vdb5
144       324     48     0     36   1       9       9      ARP_Private_Cachep
0         0       32     0     42   1       0       0      ARP_Vlan_Cachep
```

图 6-90　内存占用情况

```
[GDSZ-PS-ISG04-FW01-probe]dis sys inter kernel mem pool name kmalloc-128
Active    Number  Size   Align Slab Pg/Slab ASlabs  NSlabs Name
8927280   8927562 128    8     42   2       212560  212561 kmalloc-128

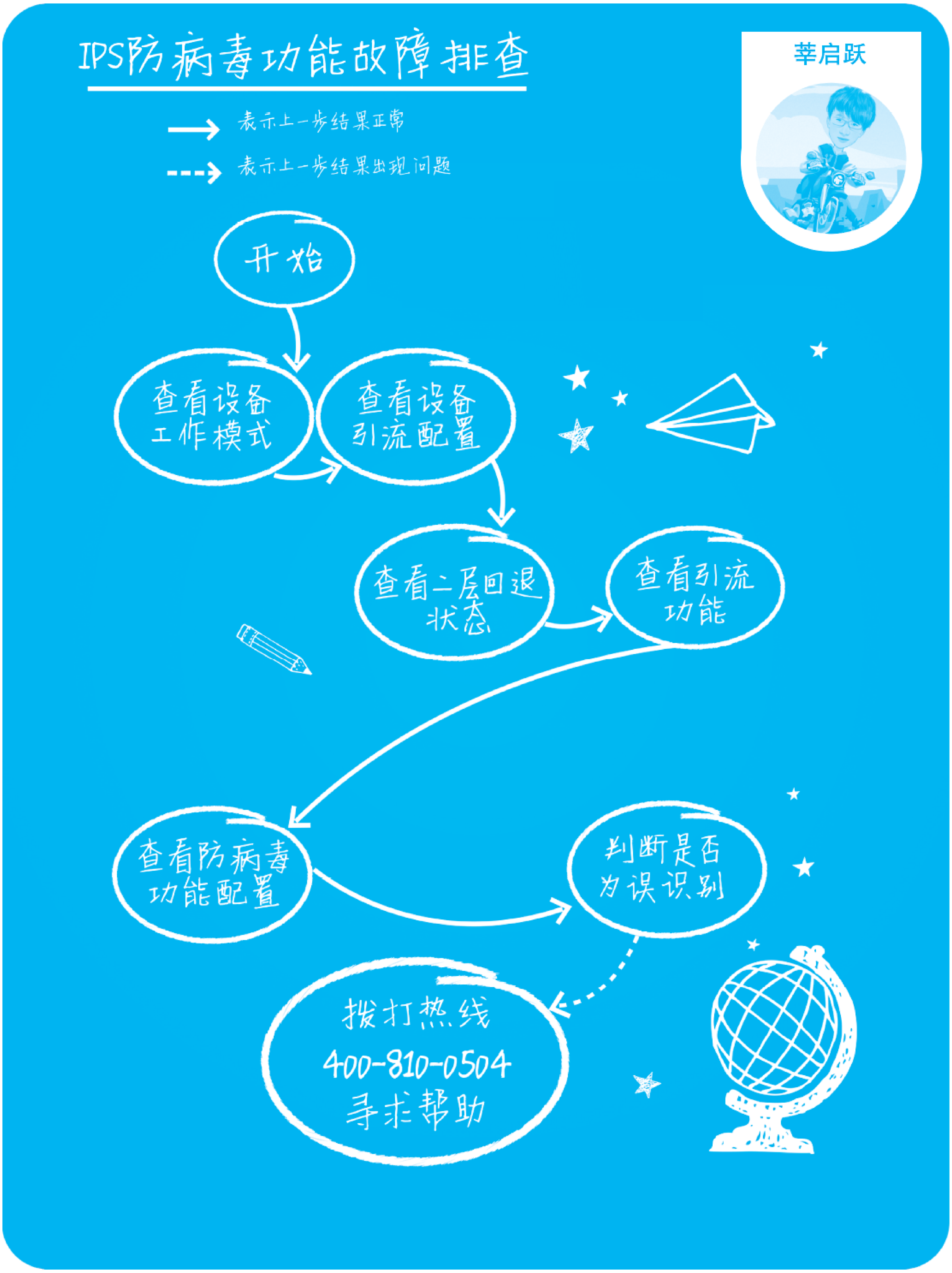
Allocation list:
Tag          Number
0x6080004    1
0xf100000    79
0x2300000    394
0xf2f0000    8925023
```

图 6-91　内存池内存明细

举例：通过 display version 命令来查看某个板卡是否发生重启，重启原因如果是内存问题会显示“Memory exhaust”。

```
<M9000>display version
H3CComware Software, Version 7.1.054, Release 9115P04
Copyright (c) 2004-2015 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
...
LPU Chassis 1 Slot 1:
Uptime is 2 weeks,1 day,18 hours,39 minutes
H3CSecPath M9010 LPU with 1 XLS408 Processor
BOARD TYPE:          NSQ1GP24TXEA0
DRAM:                1024M bytes
FLASH:               0M bytes
NVRAM:               0K bytes
PCB 1 Version:       VER.B
Bootrom Version:     511
```

```
CPLD 1 Version:        003
CPLD 2 Version:        002
Release Version:       H3CSecPath M9010-9115P04
PatchVersion    :      None
RebootCause     :      Memory exhaust
...
```


IPS防病毒功能故障排查
表示上一步结果正常
表示上一步结果出现问题
莘启跃
开始
查看设备工作模式
查看设备引流配置
查看二层回退状态
查看引流功能
查看防病毒功能配置
判断是否为误识别
拨打热线
400-810-0504
寻求帮助

06 安全产品 > 6.2 防火墙 > 6.2.14 IPS 防病毒功能故障排查 > 步骤详解

1. 开始

防病毒设备上的防病毒业务以在线方式运行于网络主干上。通过采用实时分析，自动阻截携带病毒的报文与异常流量。针对这些异常流量，通常施以阻截、隔离或干扰的处置，以预防病毒在网络中传播。可以通过配置策略实现实时分析、检测网络流量并执行定义的动作。

IPS 防病毒功能定位问题的思路是：通过查看设备工作模式，引流配置，确认设备二层回退状态，查看防病毒功能配置，是否存在误识别等步骤逐步排查，确认问题所在。

2. 流程图相关操作说明

(1) 查看设备工作模式

通过登录 IPS 插卡，查看设备目前的工作模式：直连或者旁路。如果为旁路部署，需修改为直连部署。

例如：通过 Web 页面查看 IPS 当前工作模式，如图 6-92 所示。



图 6-92 设备工作模式

通过 Web 页面，可以查看到连接模式处于直连模式，应用模式为完整功能集，在此情况下，IPS 防病毒功能才能生效。

(2) 查看设备引流配置

通过登录 IPS 插卡，查看设备安全域配置，确认设备内部域接口和外部域接口选择无错误。

例如：通过 Web 页面查看，内部域所选端口为连接内网端口，外部域所选端口为连接外部域端口，如图 6-93 和图 6-94 所示。



图 6-93 设备引流配置(1)

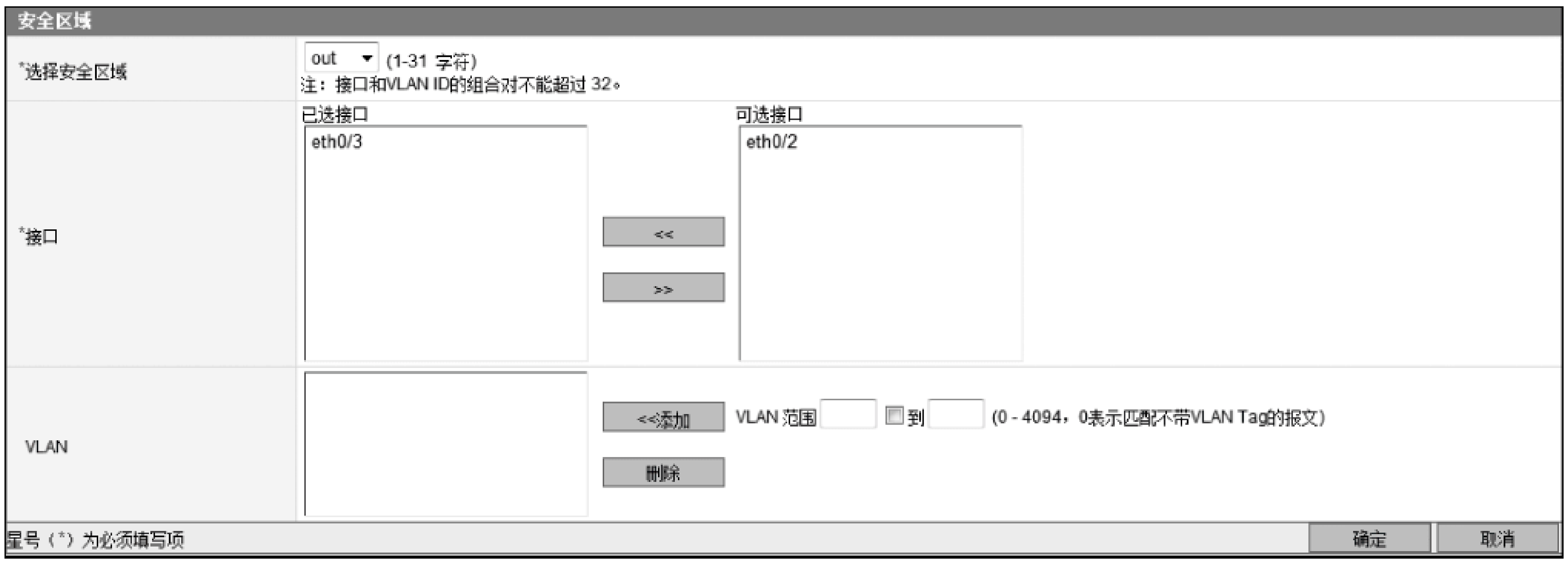


图 6-94　设备引流配置(2)

由图 6-93 和图 6-94 可以看出内部域端口定义为 Eth0/2，外部域端口定义为 Eth0/3。

查看 IPS 上段配置，确认内部域以及外部域成功关联，并正确调用。

例如：通过 IPS 插卡的 Web 页面，查看 IPS 插卡段配置，如图 6-95 所示。

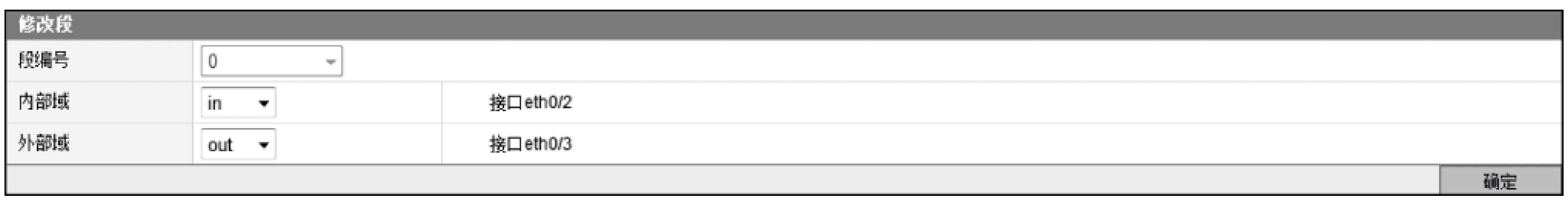


图 6-95　IPS 插卡段配置

如图 6-95 所示，通过查看段配置，确认内部域为 in，接口为 Eth0/2，外部域为 out，接口为 Eth0/3，关联段为 0。

(3) 查看二层回退状态

查看 IPS 插卡二层回退状态，确认设备处在正常工作状态。

例如：通过 Web 页面，查看设备二层回退状态，设备是否使能了二层回退，如图 6-96 所示。

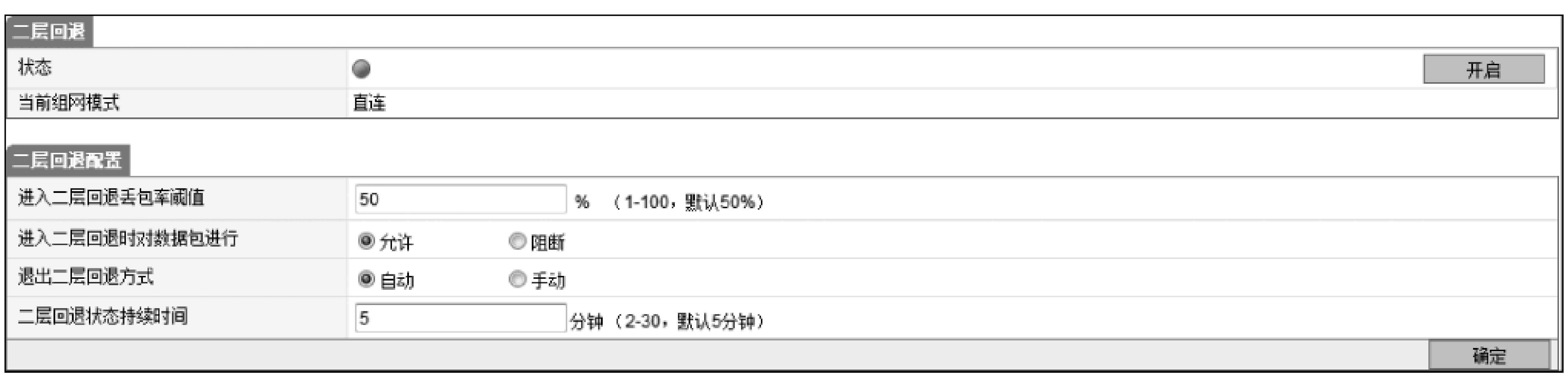


图 6-96　二层回退状态

如图 6-96 所示，通过查看设备二层回退状态，确认设备未使能二层回退功能，当前设备处于正常工作模式。

(4) 查看引流功能

防病毒功能要求双向流量都经过设备才能成功生效。如果是单向流，会导致防病毒不生效。因此，首先要检查双向流量是否引到设备上。

① "大概看"。在导航栏中单击"报表"→"报文统计"命令可以看到单向的实时报文统计，如果段的双向都有报文统计，说明双向流量大概都引到了设备上，如图 6-97 和图 6-98 所示。

② "仔细看"。在导航栏中单击"带宽管理"→"策略管理"命令，新建策略应用，默认规则



图 6-97 实时报文分布

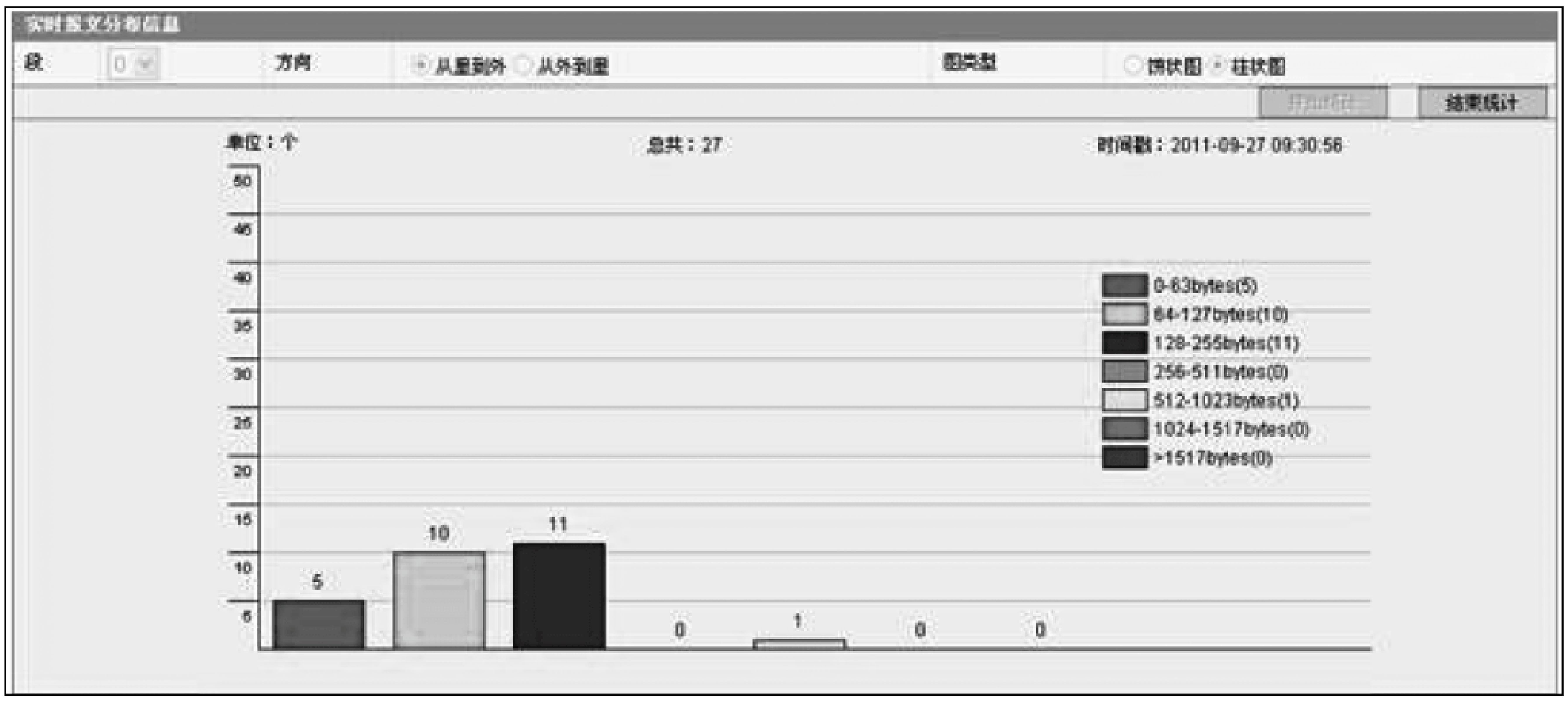


图 6-98 实时报文统计



图 6-99 检测流量应用

工作选择“permit＋notify”选项，通过带宽管理检测所有流量应用。在日志中过滤出想要的五元组日志，可以看到访问网站的流量是否双向被检测到，如果检测到则说明双向引流成功，如图 6-99 所示。

(5) 查看防病毒功能配置

查看 IPS 防病毒功能配置，确认是否开启对应病毒检测规则。

例如：通过查看 IPS 的 Web 页面，查看防病毒功能策略规则开启情况，如图 6-100 所示。

建议按照保护对象开启相应规则，默认情况下有推荐开启规则，也可以自行设定全部使能。

此外，还需注意策略应用范围，注意匹配的段和地址范围是否正确，如图 6-101 所示。

同时，配置完毕后别忘了激活。



图 6-100　防病毒功能策略规则



图 6-101　策略应用范围

(6) 判断是否为误识别

防病毒功能借助于病毒特征库的不断更新，以识别新的病毒。因此，如果特征库较老，有可能存在误识别的情况。

如果在特征库最新的情况下，产生误识别(主要是正常流量被防病毒功能阻断造成业务影响)，请收集以下信息反馈分析。

收集方法如下。

① 配置测试 IP，如本机测试 IP 地址并应用于段策略中，如图 6-102 和图 6-103 所示。

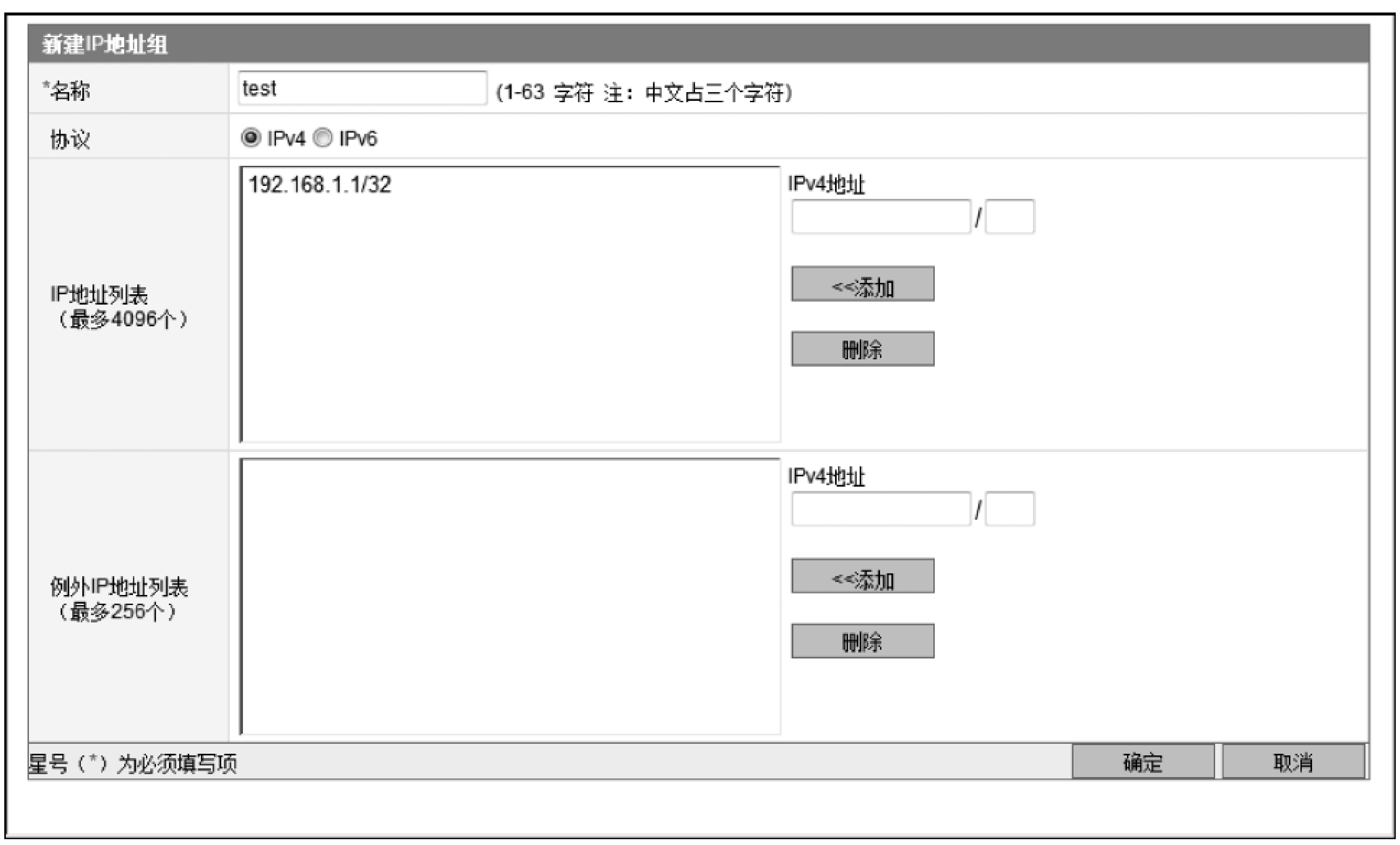


图 6-102　新建 IP 地址组



图 6-103　策略应用范围

② 策略中可疑规则动作配置为“阻断＋记录日志”，如果不清楚是哪条规则，在性能允许的情况下可以全部开启测试，如图 6-104 所示。

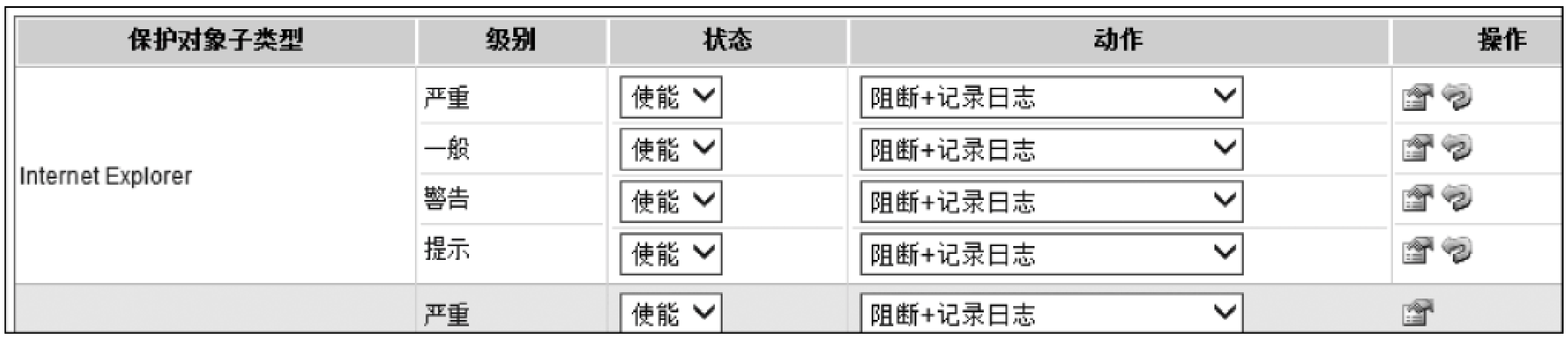


图 6-104　设置策略

③ 策略激活后，进行“问题”业务访问。测试时，建议其他功能关闭或者放通，之后导出防病毒日志，如图 6-105 所示。



图 6-105　导出防病毒日志

④ 记录设备特征库版本信息，如图 6-106 所示。



图 6-106　设备特征库版本

⑤ 记录设备 License 信息，如图 6-107 所示。



图 6-107　设备 License 信息

⑥ 测试业务流量抓包收集，流量最好不要夹杂其他业务，尽量“干净”。

抓包文件生成后，一并反馈总部处理。


IPS防攻击功能故障排查
表示上一步结果正常
表示上一步结果出现问题
莘启跃
开始
查看设备工作模式
查看设备引流配置
查看引流功能
查看二层回退状态
查看防攻击配置
判断是否为误识别
拨打热线
400-810-0504
寻求帮助

06 安全产品 > 6.2 防火墙 > 6.2.15 IPS 防攻击功能故障排查 > 步骤详解

1. 开始

IPS 对数据流进行重组和分析，一旦和设备的攻击特征规则匹配，就根据对应的规则进行告警或者阻断。并且可以根据保护对象制定专业化的防护策略。

IPS 防攻击定位故障的思路是，通过查看设备工作模式，引流配置，确认设备二层回退状态，查看 IPS 防攻击具体配置等步骤逐步排查，确认问题所在。

2. 流程图相关操作说明

(1) 查看设备工作模式

通过登录 IPS 插卡，查看设备目前的工作模式：直连或者旁路。如果为旁路部署，需修改为直连部署。

例如：通过 Web 页面查看 IPS 当前工作模式，如图 6-108 所示，路径："系统管理→设备管理→工作模式"。



图 6-108 工作模式

通过 Web 页面，可以查看到连接模式处于直连模式，应用模式为完整功能集，在此情况下，IPS 攻击防范策略才能生效。

(2) 查看引流配置

通过登录 IPS 插卡，查看设备安全域配置，确认设备内部域接口和外部域接口选择无错误。

例如：通过 Web 页面查看，内部域所选端口为连接内网端口，外部域所选端口为连接外网端口，分别如图 6-109 和图 6-110 所示。



图 6-109 连接内网端口

由图 6-109 和图 6-110 可以看出内部域端口定义为 eth0/2，外部域端口定义为 eth0/3。

查看 IPS 上段配置，确认内部域以及外部域成功关联，并正确调用。

例如：通过 IPS 插卡的 Web 页面，查看 IPS 插卡段配置，如图 6-111 所示。

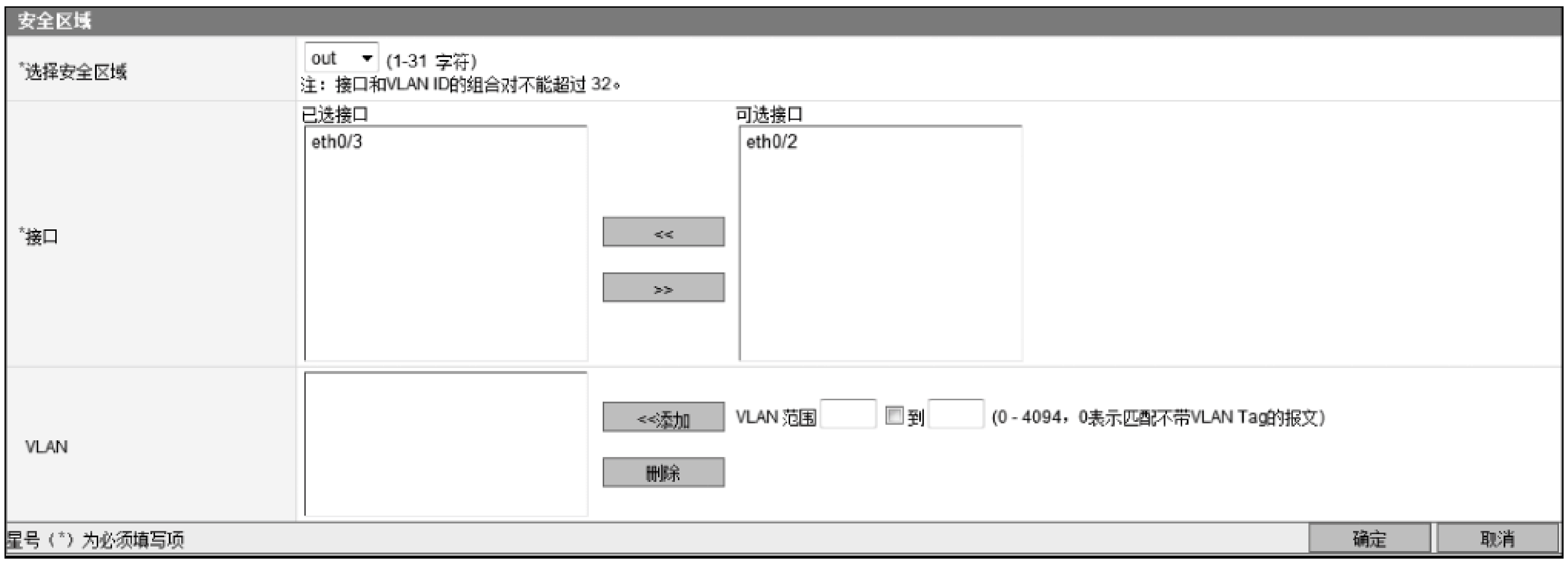


图 6-110　连接外网端口

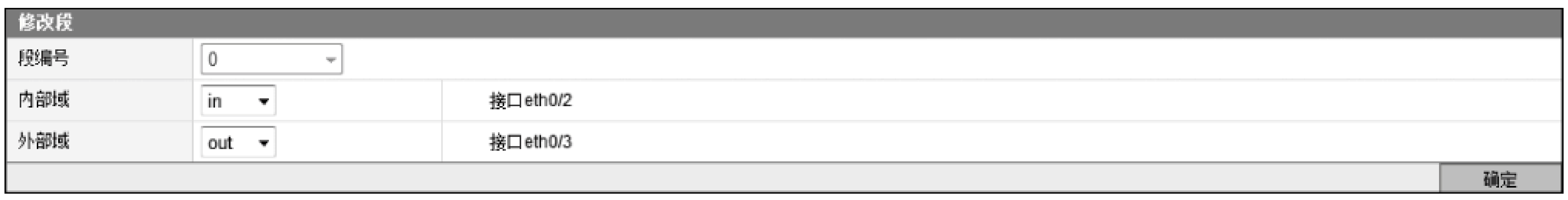


图 6-111　IPS 插卡段配置

如图 6-112 所示，通过查看段配置，确认内部域为 in，接口为 eth0/2，外部域为 out，接口为 eth0/3，关联段为 0。

（3）查看二层回退状态

查看 IPS 插卡二层回退状态，确认设备处在正常工作状态。

例如：通过 Web 页面，查看设备二层回退状态，设备是否使能了二层回退，如图 6-112 所示。路径：“系统管理→设备管理→高可靠性→二层回退”。

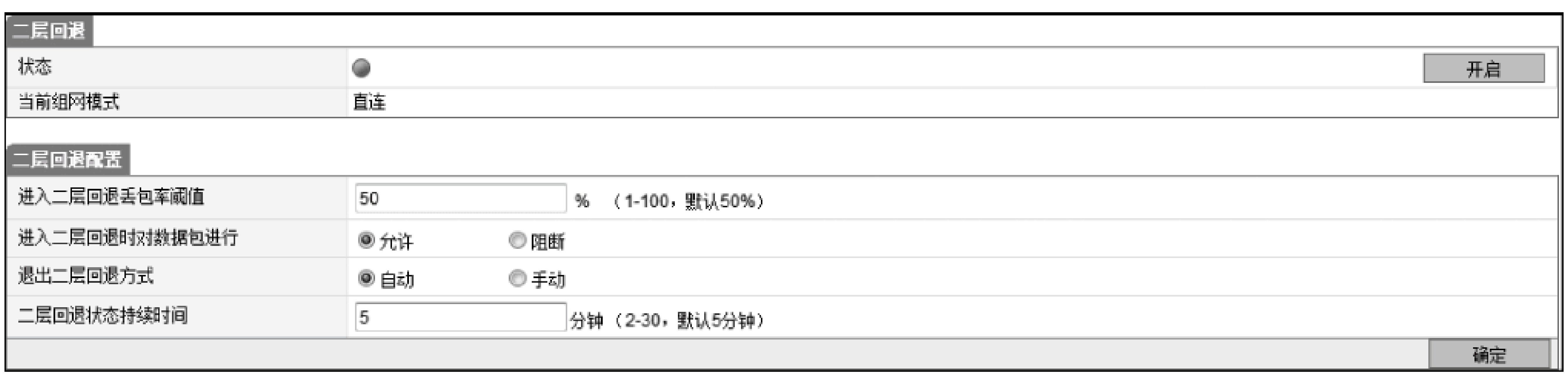


图 6-112　二层回退状态

通过查看设备二层回退状态，确认设备未使能二层回退功能，当前设备处于正常工作模式。

（4）查看引流功能

IPS 防攻击功能要求双向流量都经过设备才能生效。如果是单向流，会导致部分或者全部 IPS 防攻击出现问题。因此，首先要检查双向流量是否引到设备上。

例如：在导航栏中单击“报表”→“报文统计”命令可以看到单向的实时报文统计，如果段的双向都有报文统计，说明双向流量大概都引到了设备上，如图 6-113 和图 6-114 所示。

（5）查看防攻击配置

① 在导航栏中单击“IPS”→“策略管理”命令，进入 IPS 策略的显示页面，如图 6-115 所示。

② 单击“新建策略应用”按钮，进入新建 IPS 策略应用的配置页面，如图 6-116 所示。



图 6-113　实时报文分布

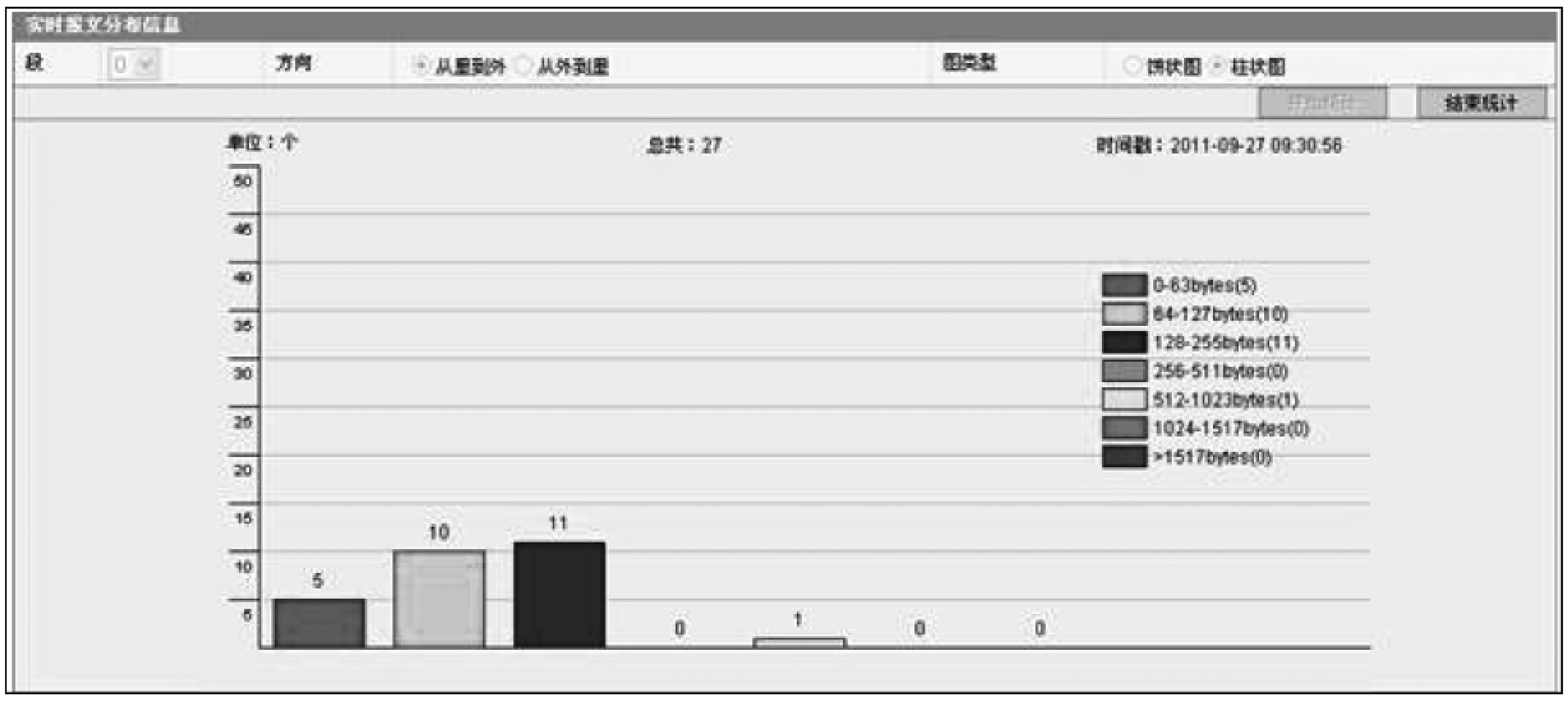


图 6-114　实时报文统计



图 6-115　IPS 策略显示页面



图 6-116　IPS 策略应用配置页面

③ 在“策略应用范围”中显示该策略的所有应用范围，可以直接在列表中对应用范围的参数进行修改。

④ 单击“新建”按钮，列表中将新增一条应用范围表项，可以直接在列表中对策略应用范围进行配置，如图 6-117 所示。



图 6-117　新建应用范围表项

⑤ 单击 图标，弹出相应表项的高级配置页面，如图 6-118 所示，可以对策略应用范围进行高级配置(可以配置多个内/外部域 IP 地址组)。



图 6-118　高级配置页面

⑥ 例如：通过查看 IPS 的 Web 页面，查看 IPS 防攻击策略调用地址情况，如图 6-119 所示。



图 6-119　IPS 防攻击策略调用地址

⑦ 然后激活策略。

(6) 判断是否为误识别

① 单击“规则管理”选项，选择所配置的策略，查询出所有的规则并选中所有规则，如图 6-120 所示。



图 6-120　规则管理

② 单击“修改查询出的所有规则”选项，选择“允许＋记录日志＋Packet Trace”选项，单击“修改动作”按钮，然后单击“激活”按钮，如图 6-121 所示。

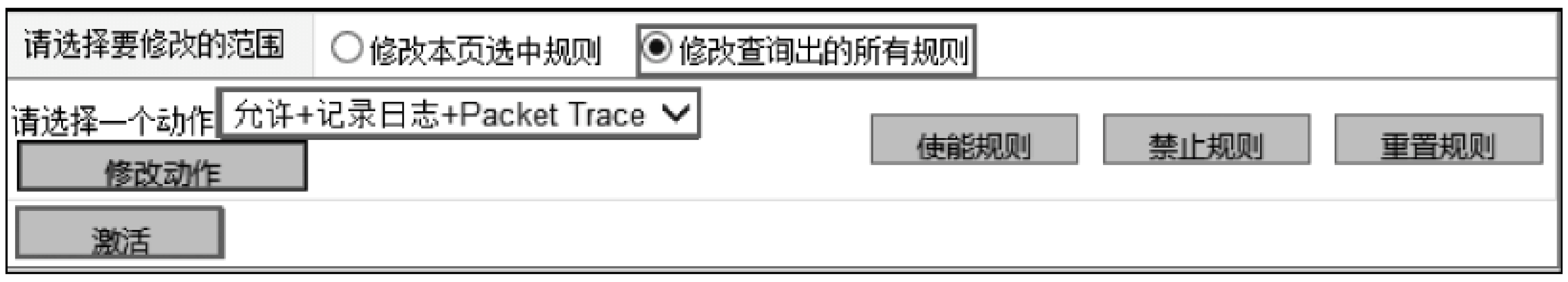


图 6-121　修改规则

③ 策略激活后，进行误识别的业务访问，导出攻击日志，并下载日志中的 Packet 文件，如图 6-122 所示。



图 6-122　导出日志

④ 记录设备特征库版本信息，如图 6-123 所示。



图 6-123　设备特征库版本

⑤ 记录设备 License 信息，如图 6-124 所示。

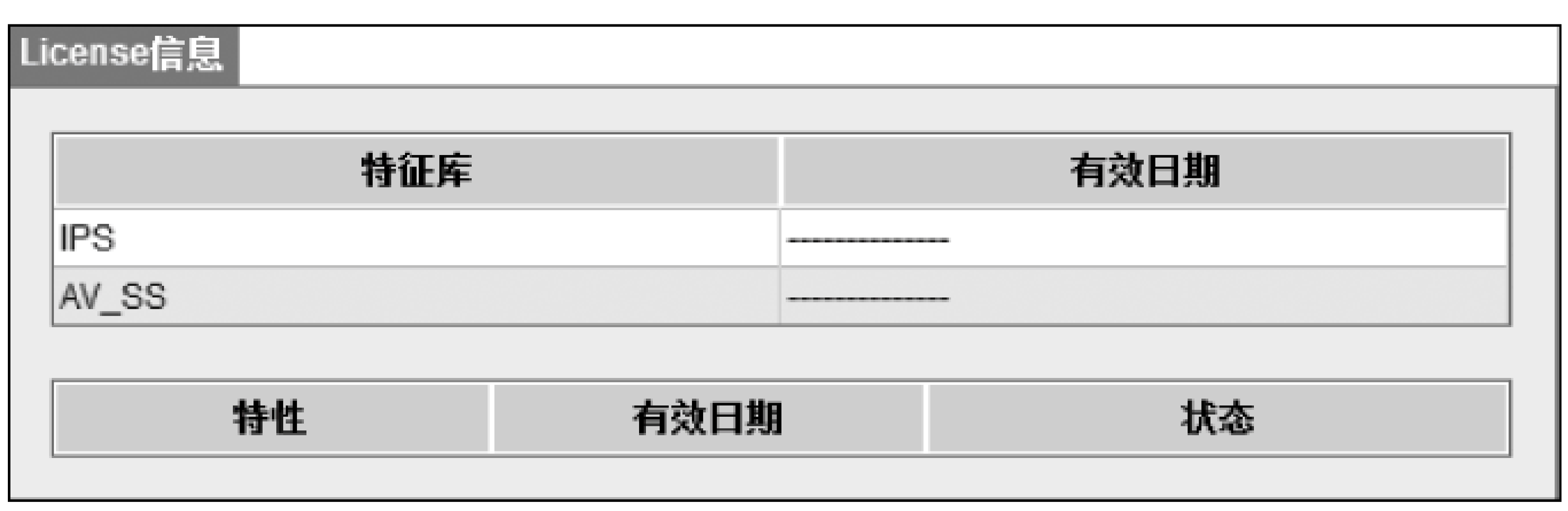
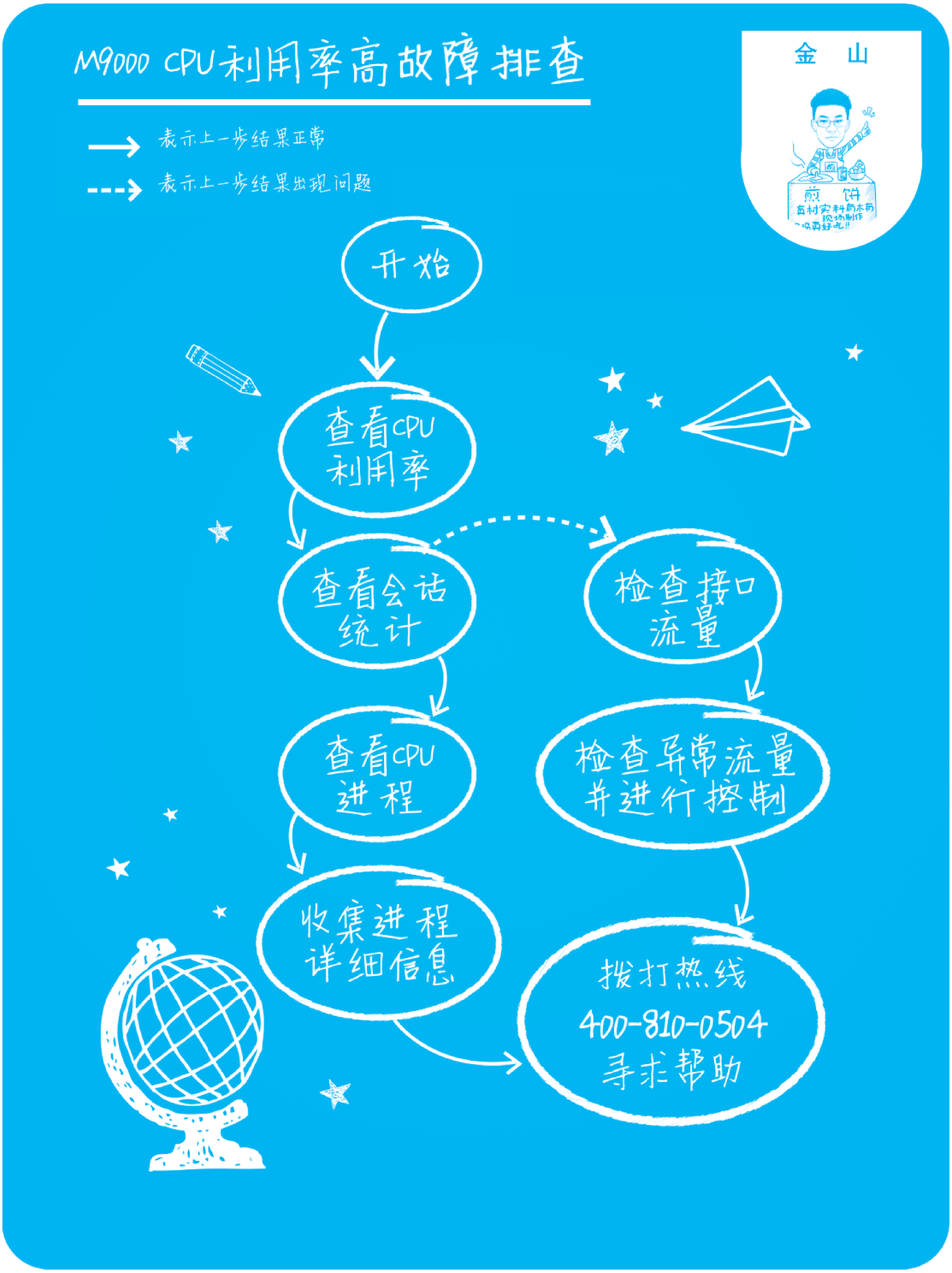


图 6-124　设备 License 信息

⑥ 记录误识别应用，包括具体的版本号。

记录输出后，一并反馈总部处理。


M9000 CPU利用率高故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
开始
查看CPU利用率
查看会话统计
检查接口流量
查看CPU进程
检查异常流量并进行控制
收集进程详细信息
拨打热线 400-810-0504 寻求帮助

1. 开始

M9000 CPU 利用率高问题定位故障的思路是：首先检查设备 CPU 利用率数值是否正常，由于 M9000 基于全分布式硬件架构设计，主控板、接口板、交换网板、安全业务板均有各自的 CPU，因此要先确认具体是哪一块单板的 CPU 利用率出现偏高；然后检查当前整机会话数统计值，是否与日常运维观察的正常业务运行时统计值相符。如果 M9000 当前的会话新建连接速率和并发连接数统计值正常，应进一步查找引起相应槽位 CPU 利用率高的进程，并收集相关信息后反馈；如果 M9000 当前的会话新建连接速率和并发连接数统计值远远大于日常运维观察的数值，则说明当前 M9000 上很可能存在某种异常流量，建议先根据端口统计数据查找异常流量的接收端口，再根据会话表信息判断异常流量的具体特征，溯源并消除，最终恢复 M9000 的 CPU 使用情况。

2. 流程图相关操作说明

(1) 查看 CPU 利用率

通过命令查看 M9000 各单板 CPU 利用率统计数据。可查询的单板主要有主控板、交换网板、接口板、安全业务板等几类。每个安全业务板(目前仅防火墙业务板一种)包含两个 CPU，CPU 0 对应后插板的控制平面 CPU，与接口板 CPU 的功能基本一致；CPU 1 对应前插板的数据平面 CPU，主要实现安全业务处理、数据转发等功能。除安全业务板以外，其他单板均只含有一个 CPU。当设备无业务负载时，通常主控板 CPU 利用率维持在 5%左右，交换网板 CPU 利用率维持在 10%左右，其余各 CPU 利用率数据一般在 5%以下。

实际运维过程中，设备 CPU 利用率一般会通过网管系统实时监控，若发现 M9000 某 CPU 利用率持续偏高，远大于系统监控告警阈值，应注意先检查具体是哪个 CPU 利用率出现过高的现象。若检查确认是安全业务板 CPU 1 利用率高，多数情况是由于 M9000 接收到了较大的业务流量或其他异常流量造成，若检查确认是其余 CPU 出现利用率高，则可能是其他原因造成，需要进一步排查分析。

命令：*display cpu-usage*

例如：通过命令查看 M9000 各 CPU 利用率情况，其中 1 号框 7 号槽位防火墙业务板 CPU 1 利用率达到了 87%左右，这个数值也是安全业务板 CPU 1 在实际运行过程中可能达到的最大数值，因此可以断定当前 1 号框 7 号槽位防火墙业务板性能压力非常大，具体原因很可能是较大的业务流量或其他异常流量导致，须立即进一步排查分析。

```
<H3C>display cpu-usage
Chassis 1 Slot 1 CPU 0 CPU usage:
        2% in last 5 seconds
        2% in last 1 minute
        2% in last 5 minutes

Chassis 1 Slot 4 CPU 0 CPU usage:
        6% in last 5 seconds
        5% in last 1 minute
        6% in last 5 minutes
```

```
Chassis 1 Slot 7 CPU 0 CPU usage:
        1% in last 5 seconds
        1% in last 1 minute
        1% in last 5 minutes

Chassis 1 Slot 7 CPU 1 CPU usage:
       87% in last 5 seconds
       87% in last 1 minute
       86% in last 5 minutes

Chassis 1 Slot 10 CPU 0 CPU usage:
       10% in last 5 seconds
       10% in last 1 minute
       10% in last 5 minutes

Chassis 1 Slot 11 CPU 0 CPU usage:
        9% in last 5 seconds
       10% in last 1 minute
       10% in last 5 minutes

Chassis 1 Slot 12 CPU 0 CPU usage:
       10% in last 5 seconds
       10% in last 1 minute
       10% in last 5 minutes

Chassis 1 Slot 13 CPU 0 CPU usage:
        9% in last 5 seconds
       10% in last 1 minute
       10% in last 5 minutes
```

（2）查看会话统计

M9000 在线运行过程中，如果其接收的流量在短时间内创建大量会话，势必会极大地消耗主控板和安全业务板的 CPU 资源，因此需在问题现象发生时，检查主控板及安全业务板的会话统计信息是否存在异常。如果会话统计信息中的会话数、会话新建速率等与日常运维观察值相比增加很多，甚至达到了设备软件规格值，则可以判定 CPU 利用率高问题便是由此引起，可通过进一步查看会话表项明细或抓包等方法确认异常流量的具体情况。如果会话统计信息中的各项数值与日常运维值相差不大，则应进一步检查具体是哪个 CPU 进程引起利用率高。

命令：*display session statistics summary*

例如：通过命令查看 M9000 会话统计信息，命令回显数据将包括所有的主控板和安全业务板数据。“Session”列对应当前业务流量在相应槽位单板上创建的总的会话数，“Rate”列对应相应的新建会话速率。从本例中不难看出，M9000 1 号框 7 号槽位防火墙业务板当前并发连接数已经超过 1300 万，每秒 TCP 会话新建连接速率超过 17 万，远高于日常值，可以判定当前 M9000 正受到 TCP 泛洪异常流量影响。

```
<H3C>display session statistics summary
Chassis Slot CPU Sessions TCP       UDP      Rate      TCP rate  UDP rate
1       4    0   2        2         0        0/s       0/s       0/s
1       7    1   13547855 13543080  4775     175520/s  175242/s  278/s
2       4    0   0        0         0        0/s       0/s       0/s
2       7    1   0        0         0        0/s       0/s       0/s
```

(3) 查看 CPU 进程

检查出现利用率高的 CPU 运行进程情况,先查找具体是哪个进程占用了较多的 CPU 资源,再对相应的软件模块进行排查。例如,若系统日志进程占用 CPU 较多,则应进一步排查是否设备在问题发生时产生了过多的日志信息或其他异常情况;若 Telnet 进程占用 CPU 较多,则应进一步排查是否设备接受了过多的 Telnet 远程连接请求或其他异常情况。表 6-1 是 M9000 部分常见进程与各软件功能特性的对应关系,通过对照确认占用 CPU 多的是哪个进程后,即可重点对相应的功能特性进行排查。

表 6-1 M9000 部分常见进程与各软件功能特性对应表

diagd	设备监控管理
fsd/dfsd	文件系统管理
had	双机热备管理与维护
syslogd	维护日志管理
pdtpowfanmanage	系统风扇管理
mdcd	Context 虚拟设备管理与维护
ifmgr	设备接口管理
sysmand	设备基本配置文件管理
edev	设备硬件资源管理
lauthd	本地认证,负责接收发送认证报文
aaad	AAA 子系统
laggd	链路聚合管理
tranged	Timerange 功能模块
vland	VLAN 功能模块
aclmgrd	ACL 功能模块
routed	IPv4 路由管理
usrd	静态路由管理
qosd	QoS 管理
bftpd	分布式文件系统管理
lods	接口板软件版本加载服务器
telnetd	Telnet 服务
login	用户认证管理,认证通过后启动 comsh
comsh	命令行解析服务
oapd	OAP 服务
coppd	控制平面协议报文上送速率限制服务
ttymgrd	TTY 管理
licd	LICENSE 管理
tunneld	Tunnel 接口管理模块
rtermcond	远程终端接入
portald	Portal 服务
portalproxyd	Portal Proxy 服务
atkd	uRPF 等功能
sessiond	会话管理、连接数限制、状态防火墙等功能
aprd	APR 应用层协议识别功能
objpd	域间对象策略
macsecd	MACsec 功能

续表

portsecd	端口安全、dot1x、MAC 地址认证功能
natd	NAT 网络地址转换服务
ipsecd	IPSec 服务
iked	IKE 服务

命令：*display process cpu chassis x slot x cpu x*

例如：通过命令查看 M9000 1 号框 4 号槽位主控板各进程 CPU 利用率情况，可以看到路由管理进程始终占用了大量的 CPU 资源，说明 M9000 的路由表维护部分可能存在异常，须进一步排查是否学习到了大量的路由条目且持续震荡等问题。

```
<H3C>display process cpu chassis 1 slot 4 cpu 0
CPU utilization in 5 secs:70.7%; 1 min: 68.5%; 5 mins: 69.4%
    429     0.0%     0.0%     0.0%     telnetd
    430     0.0%     0.0%     0.0%     dnsd
    516     0.0%     0.0%     0.0%     natd
    570     0.0%     0.0%     0.0%     ipstackd
    571     0.0%     0.0%     0.0%     [karp/1]
    572     0.0%     0.0%     0.0%     [kwadj/1]
    573     0.0%     0.0%     0.0%     [kfib/1]
    578     57.0%    55.2%    56.7%    routed
    582     0.0%     0.0%     0.0%     usrd
    593     0.0%     0.0%     0.0%     seczoned
    639     0.0%     0.0%     0.0%     objpd
    690     0.0%     0.0%     0.0%     telnetd
    792     0.0%     0.0%     0.0%     atkd
   1464     0.0%     0.0%     0.0%     sessiond
   1596     0.0%     0.0%     0.0%     [krpc_recv]
   1597     0.0%     0.0%     0.0%     [krpc_recv]
   1627     0.0%     0.0%     0.0%     [krpc_recv]
   1629     0.0%     0.0%     0.0%     [krpc_recv]
   1631     0.0%     0.0%     0.0%     [krpc_recv]
   1636     0.0%     0.0%     0.0%     [krpc_recv]
   1637     0.0%     0.0%     0.0%     [krpc_recv]
   1648     0.0%     0.0%     0.0%     [krpc_recv]
   1653     0.0%     0.0%     0.0%     [krpc_recv]
   1745     0.0%     0.0%     0.0%     trackd
   2263     0.0%     0.0%     0.0%     [krpc_recv]
   2507     0.0%     0.0%     0.0%     snmpd
   2765     0.0%     0.0%     0.0%     telnetd
   2766     0.0%     0.0%     0.0%     login
   2768     0.0%     0.0%     0.0%     comshc
   2769     0.0%     0.0%     0.0%     comsh
   2884     0.0%     0.0%     0.0%     telnetd
   2885     0.0%     0.0%     0.0%     login
   2887     0.0%     0.0%     0.0%     comshc
   2888     0.0%     0.0%     0.0%     comsh
   3042     0.0%     0.0%     0.0%     getty
   3043     0.0%     0.0%     0.0%     login
   3045     0.0%     0.0%     0.0%     comshc
   3046     0.0%     0.0%     0.0%     comsh
```

（4）收集进程详细信息

如果工程师无法根据前述方法排除现场问题，可在 CPU 利用高问题发生时，即时收集记录 CPU 进程相关详细信息并反馈技术支持中心协助处理。

命令：*display process cpu chassis x slot x cpu x*

display processjob x chassis x slot x cpu x

follow job x

例如：以“scmd”进程为例，收集相关详细信息。

① 查看“scmd”进程对应的任务 ID(JID)。

```
<H3C>display process cpu chassis 1 slot 4 cpu 0
CPU utilization in 5 secs: 0.6%; 1 min: 0.5%; 5 mins: 0.5%
    JID      5Sec      1Min      5Min      Name
      1      0.0%      0.0%      0.0%      scmd
      2      0.0%      0.0%      0.0%      [kthreadd]
      3      0.0%      0.0%      0.0%      [migration/0]
      4      0.0%      0.0%      0.0%      [ksoftirqd/0]
      5      0.0%      0.0%      0.0%      [watchdog/0]
      6      0.0%      0.0%      0.0%      [migration/1]
      7      0.0%      0.0%      0.0%      [ksoftirqd/1]
      8      0.0%      0.0%      0.0%      [watchdog/1]
      9      0.0%      0.0%      0.0%      [migration/2]
     10      0.0%      0.0%      0.0%      [ksoftirqd/2]
     11      0.0%      0.0%      0.0%      [watchdog/2]
     12      0.0%      0.0%      0.0%      [migration/3]
     13      0.0%      0.0%      0.0%      [ksoftirqd/3]
     14      0.0%      0.0%      0.0%      [watchdog/3]
     15      0.0%      0.0%      0.0%      [migration/4]
     16      0.0%      0.0%      0.0%      [ksoftirqd/4]
     17      0.0%      0.0%      0.0%      [watchdog/4]
     18      0.0%      0.0%      0.0%      [migration/5]
     19      0.0%      0.0%      0.0%      [ksoftirqd/5]
     20      0.0%      0.0%      0.0%      [watchdog/5]
     21      0.0%      0.0%      0.0%      [migration/6]
     22      0.0%      0.0%      0.0%      [ksoftirqd/6]
     23      0.0%      0.0%      0.0%      [watchdog/6]
     24      0.0%      0.0%      0.0%      [migration/7]
     25      0.0%      0.0%      0.0%      [ksoftirqd/7]
     26      0.0%      0.0%      0.0%      [watchdog/7]
     27      0.0%      0.0%      0.0%      [migration/8]
     28      0.0%      0.0%      0.0%      [ksoftirqd/8]
     29      0.0%      0.0%      0.0%      [watchdog/8]
     30      0.0%      0.0%      0.0%      [migration/9]
     31      0.0%      0.0%      0.0%      [ksoftirqd/9]
```

② 根据任务 ID 查看进程摘要信息。

```
<H3C>display process job 1 chassis 1 slot 4 cpu 0
                        Job ID: 1
                           PID: 1
                    Parent JID: 0
                    Parent PID: 0
```

```
                Executable path : /sbin/scmd
                       Instance : 0
                        Respawn : OFF
                  Respawn count : 1
          Max. spawns per minute : 0
                   Last started : Tue Mar  3 06:35:01 2015
                  Process state : sleeping
                      Max. core : 0
                           ARGS : -
  TID   LAST_CPU    Stack    PRI    State   HH:MM:SS:MESC   Name
   1       9         84K     120      S      0:0:5:680      scmd
```

③ 根据任务 ID 查看进程详细信息。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]probe
[H3C-probe]follow job 1
Attaching to process 1 (scmd)
Iteration 1 of 5
------------------------------
Thread (LWP 1):
Switch counts: 20668
User stack:
#0  0x0000005555757de4 in epoll_wait+0x1c/0x4c
#1  0x000000012001be4c in ??
Kernel stack:
[<ffffffff8049da24>] schedule+0x6c4/0xfe0
[<ffffffff8049e5e8>] schedule_timeout+0x98/0xe0
[<ffffffff80310894>] sys_epoll_wait+0x4d4/0x5a0
[<ffffffff80202f44>] stack_done_ra+0x0/0x1c

Iteration 2 of 5
------------------------------
…
```

将收集的上述信息，连同 M9000 诊断信息、logfile 日志文件一起反馈至技术支持中心。

(5) 检查接口流量

如果 M9000 的会话统计数据远大于日常运维观察值，应注意检查各业务端口接收流量是否合理，符合日常业务流量值大小。若某个端口接收到的流量值特别大，远超出日常水平，则很可能是网络中存在临时性的泛洪异常流量。若 M9000 直联服务器或 PC 机，则应当重点排查该端口下联服务器或 PC 是否感染病毒，是否有异常程序造成其向网络中大量发送报文；若该端口与其他网络设备互联，则应“顺藤摸瓜”，进一步向异常泛洪流量的来源方向排查，直至查找到流量的源头。异常泛洪流量来自内部网络的，建议尽快查找到流量源头并通过下线、修复异常程序等方式消除其对网络的影响；异常泛洪流量来自 Internet 的，可以尝试配置 M9000 的攻击防范策略进行防御，或联系 ISP 寻求更好的解决方案。

命令：*display interface GigabitEhernet x*

例如：通过命令查看接口流量，管理员发现 M9000 某端口入方向流量非常大，已经达到限速值，而出方向流量非常少，与业务系统管理员核实后确认该端口下联服务器正常情况下不

会产生如此大的流量，因此判断该流量是异常的非业务流量，需进一步溯源并消除。

```
<H3C>display interface GigabitEthernet 1/1/0/23
GigabitEthernet1/1/0/23
Current state: Up
Line protocol state: Up
Description: GigabitEthernet1/1/0/23 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet protocol processing: disabled
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 5cdd-70a3-1f7e
IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 5cdd-70a3-1f7e
Media type is twisted pair
Port hardware type is 1000_BASE_T
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Last clearing of counters: Never
 Peak value of input:125001087 bytes/sec, at 2015-03-18 02:36:54
 Peak value of output:4896 bytes/sec, at 2015-03-10 02:22:48
 Last 300 seconds input:244144 packets/sec 124799898 bytes/sec 100%
 Last 300 seconds output:3 packets/sec 1280 bytes/sec 0%
 Input (total):471140274174 packets, 68645751777 bytes
        471138069533 unicasts, 228819 broadcasts, 1975822 multicasts, 0 pauses
 Input (normal):471140274174 packets, - bytes
        471138069533 unicasts, 228819 broadcasts, 1975822 multicasts, 0 pauses
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, - overruns, 0 aborts
         - ignored, - parity errors
 Output (total):1788789 packets, 12874475 bytes
          1786559 unicasts, 485 broadcasts, 1745 multicasts, 0 pauses
 Output (normal):1788789 packets, - bytes
          1786559 unicasts, 485 broadcasts, 1745 multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, - no carrier
```

(6) 检查异常流量并进行控制

除直接对异常流量镜像抓包分析外，可以通过查看 M9000 会话表项信息来分析异常流量的特点，以便实施相应的防御措施。如果异常流量创建的会话表项目的地址、目的端口都相同，则可以通过配置域间策略或 DoS 攻击防范策略阻断；如果异常流量创建的会话表项源 IP 地址均为随机公网 IP 且发起方处于内部私网 IP 区域中，则可以通过在内网端口配置 URPF 策略阻断。总之，通过打印出一定数量的会话表项详细信息，管理员即可从中发现异常流量在 4 层及 4 层以下报文头部信息中的规律，并根据这个规律，合理配置 M9000 各项功能特性，最终实现将异常流量丢弃，且保证正常业务流转发的目的。如果异常流量来源于内部网络，更好的建议是直接排查出异常流量源头并消除。

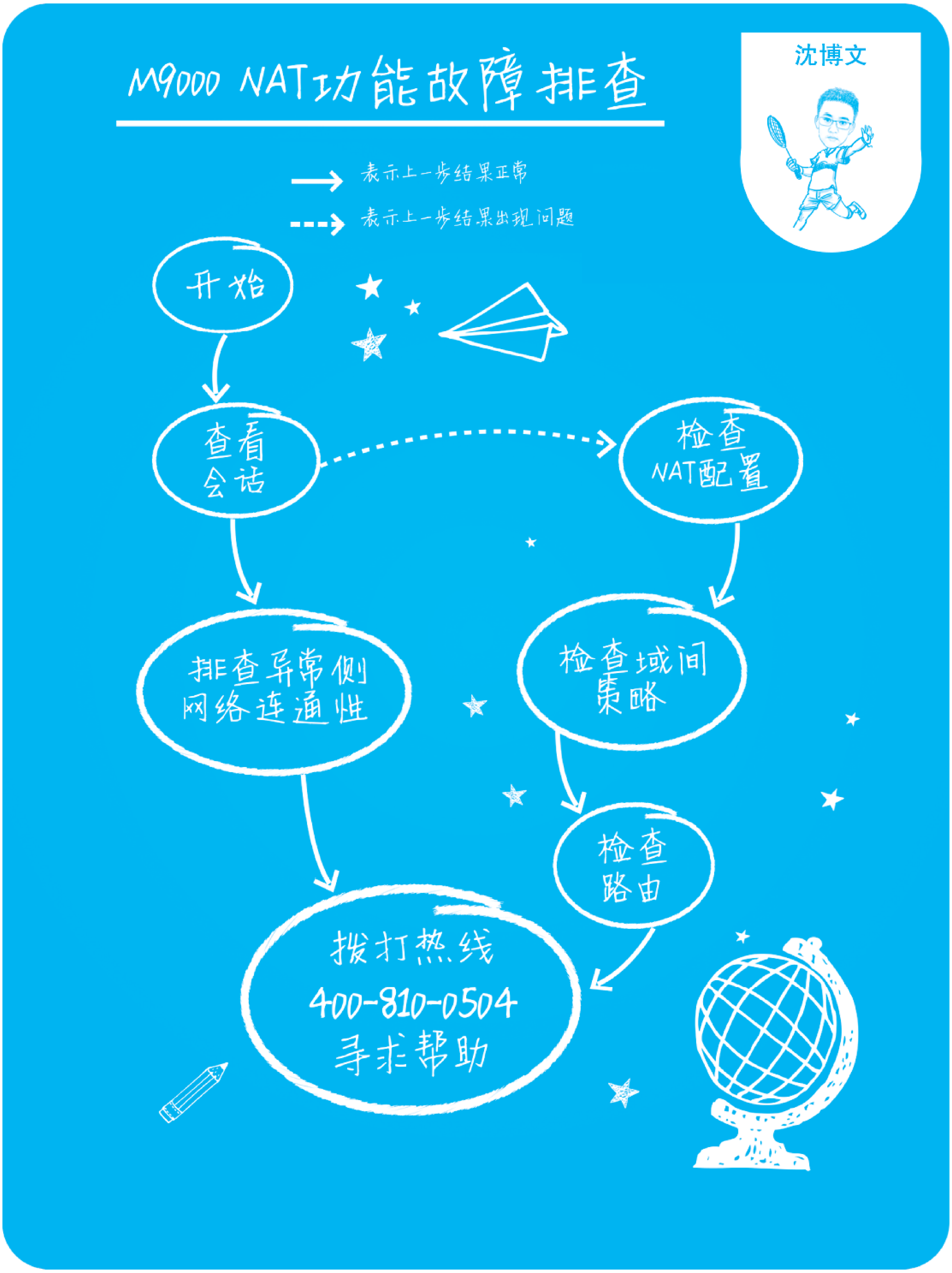
命令：*display session table ipv4 verbose*

display session table ipv6 verbose

例如：通过命令打印约100条M9000当前会话表项信息，其中约70条会话表项均为如下形式(列举两个会话表项)，不难看出源IP地址为172.31.0.1的主机向M9000发起了大量的TCP连接请求和大量的TCP SYN报文，这种异常流量属于典型的SYN Flood泛洪攻击，管理员可以先对源主机操作系统及程序进行检查，条件允许时可暂时将源主机离线以观察网络状态是否恢复；也可通过在M9000上配置域间策略、黑名单或攻击防范策略等措施阻断异常流量，减小其对其他网络设备及业务的影响。

```
<H3C>display session table ipv4 verbose
Slot 4 in chassis 1:
Initiator:
  Source      IP/port: 172.31.0.1/8709
  Destination IP/port: 172.31.0.18/23
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: M-GigabitEthernet1/0/0/0
  Source security zone: management
Responder:
  Source      IP/port: 172.31.0.18/23
  Destination IP/port: 172.31.0.1/8709
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_SYN
Application: TELNET
Start time: 2015-03-18 02:33:03   TTL:29s
Initiator->Responder:        1122 packets        71808 bytes
Responder->Initiator:           0 packets            0 bytes

Initiator:
  Source      IP/port: 172.31.0.1/8710
  Destination IP/port: 172.31.0.18/23
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: M-GigabitEthernet1/0/0/0
  Source security zone: management
Responder:
  Source      IP/port: 172.31.0.18/23
  Destination IP/port: 172.31.0.1/8710
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_SYN
Application: TELNET
Start time: 2015-03-18 02:33:03   TTL:29s
Initiator->Responder:            1118 packets        71552 bytes
Responder->Initiator:               0 packets            0 bytes
```


M9000 NAT功能故障排查
沈博文
表示上一步结果正常
表示上一步结果出现问题
开始
查看会话
检查NAT配置
排查异常侧网络连通性
检查域间策略
检查路由
拨打热线
400-810-0504
寻求帮助

1. 开始

NAT 是 M9000 最主要的功能之一，M9000 的会话记录了 NAT 转换的所有信息，排查 NAT 的问题时要结合会话查看。M9000 的 NAT 问题定位故障的思路是：先查看设备上是否有会话，如果没有会话先判断设备是否收到报文，然后依次检查设备 NAT、域间策略和路由等相关配置，确认报文转发路径正确且没有被过滤；如果设备上有会话，就检查 NAT 前后的地址是否正确，收发报文是否正常，如果收发报文不正常需要根据会话报文统计情况进一步排查内外网路由。

2. 流程图相关操作说明

(1) 查看是否有相关会话

要想确认设备是否进行了正常的 NAT 转换，最直接的方法就是查看设备的会话信息，通过详细的会话信息，查看设备是否进行了正确的转换工作。

命令：*display session table ipv4 source-ip x.x.x.x destination-ip x.x.x.x verbose*

例如：通过命令可以看到源为 192.168.5.1 的数据报文经过 M9000 进行 NAT 转换后地址变成了 60.191.66.139，报文收发也正常。

```
<H3C>display session table ipv4 source-ip 192.168.5.1 destination-ip 60.170.255.12 verbose
Slot 4 in chassis 1:
Initiator:
  Source      IP/port: 192.168.5.1/2
  Destination IP/port:60.170.255.12/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface:GigabitEthernet 1/1/0/1
  Source security zone:Trust
Responder:
  Source      IP/port:60.170.255.12/2
  Destination IP/port: 60.191.66.139/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface:GigabitEthernet 1/1/0/23
  Source security zone:Untrust
State: ICMP_REPLY
Application: OTHER
Start time: 2015-05-07 08:15:13   TTL: 17s
Initiator->Responder:          5 packets        420 bytes
Responder->Initiator:          5 packets        420 bytes
```

(2) 排查异常侧网络连通性

如果根据会话查看 M9000 地址转换正常，但是没有收到响应方的报文，需要仔细检查 M9000 到报文源目的两端地址的路由，同时也需要仔细检查内部网络或者服务器到 M9000 的路由，确保数据流的来回报文都经过 M9000。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看内网和外网的路由都正常。

```
<H3C>display ip routing-table 60.170.255.12

Summary Count :1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/0           Static  60  0           60.100.1.2      GE1/1/0/23

<H3C>display ip routing-table 172.31.0.1

Summary Count : 2

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/0           Static  60  0           60.100.1.2      GE1/1/0/23
172.31.0.0/24       Direct  0   0           192.168.100.2   GE1/1/0/1
```

（3）检查 NAT 配置

如果防火墙会话不正常，先查看 NAT 的配置是否正确。这里分以下几种情况。

① 检查 NAT Outbound 配置。

命令：*display nat outbound*

display nat address-group x

display acl xxxx

例如：通过命令查看 NAT 的地址池、ACL 规则以及下发接口是否正确，ACL 规则、ACL 的匹配次数等相关配置。

```
<H3C>display nat outbound
NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/1/0/23
    ACL: 3000           Address group: 0        Port-preserved: N
    NO-PAT: N           Reversible: N
Config status: Active

<H3C>display nat address-group 0
  Address group 0:
    Port range: 1-65535
    Address information:
      Start address         End address
      60.191.66.139         60.191.66.139

<H3C>display acl 3000
Advanced ACL  3000, named -none-, 1 rule,
ACL's step is 5
 rule 0 permit ip (27 times matched)
```

② 检查 NAT Server 配置。

命令：*display nat server*

```
<H3C>dis nat server
NAT internal server information:
  Totally 1 internal servers.
```

```
    Interface: GigabitEthernet1/1/0/23
      Protocol: 0(IPv4)
      Global IP/port: 60.100.1.3/0
      Local IP/port : 192.168.1.5/0
      Config status : Active
      Global flow-table status: Active
      Local flow-table status: Active
```

③ 检查 NAT Static 配置。

命令：*display nat static*

```
<H3C>display nat static
Static NAT mappings:
  Totally 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP      : 192.168.1.6
    Global IP     : 60.100.1.10
    Config status : Active
    Local flow-table status: Active
    Global flow-table status:
      Interface GigabitEthernet1/1/0/23 : Active

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/1/0/23
    Config status: Active
```

(4) 检查域间策略

查看安全域及域间策略，并作调整、放通。

查看防火墙设备上相关业务接口是否已经正确的加入安全域。

命令：*display security-zone name x*

例如：通过命令查看，可以确认两个业务接口已经正确加入安全域。

```
<H3C>display security-zone name trust
Name: Trust
Members:
  GigabitEthernet1/1/0/1

<H3C>display security-zone name untrust
Name: Untrust
Members:
  GigabitEthernet1/1/0/23
```

确认接口已经加入安全域后，查看相关域间策略，确保发起方区域到相应方区域的域间策略已放通，保证数据流的正常建立。

命令：*display packet-filter zone-pair security source x destination x*

display acl x

display object-policy zone-pair security source x destination x

display object-policy ip x

例如：通过命令查看，可以确认 trust 到 untrust 的域间策略已经全部放通。

```
<H3C>display packet-filter zone-pair security source trust destination untrust
Zone-pair: source Trust destination Untrust
  ACL 3000

<H3C>display acl 3000
Advanced ACL  3000, named -none-, 1 rule,
ACL's step is 5
  rule 0 permit ip (40 times matched)
```

（5）检查路由

如果防火墙 NAT 和域间策略配置都正确，但是会话不正常，可以检查下路由信息。如果完全没有会话信息，可能是设备没有收到数据报文，如果 NAT 地址转换错误，可能是报文走了不同的出接口。

命令：*display ip routing-table x.x.x.x*

例如：通过命令查看路由相关是否正确。

```
<H3C>display ip routing-table 60.170.255.12

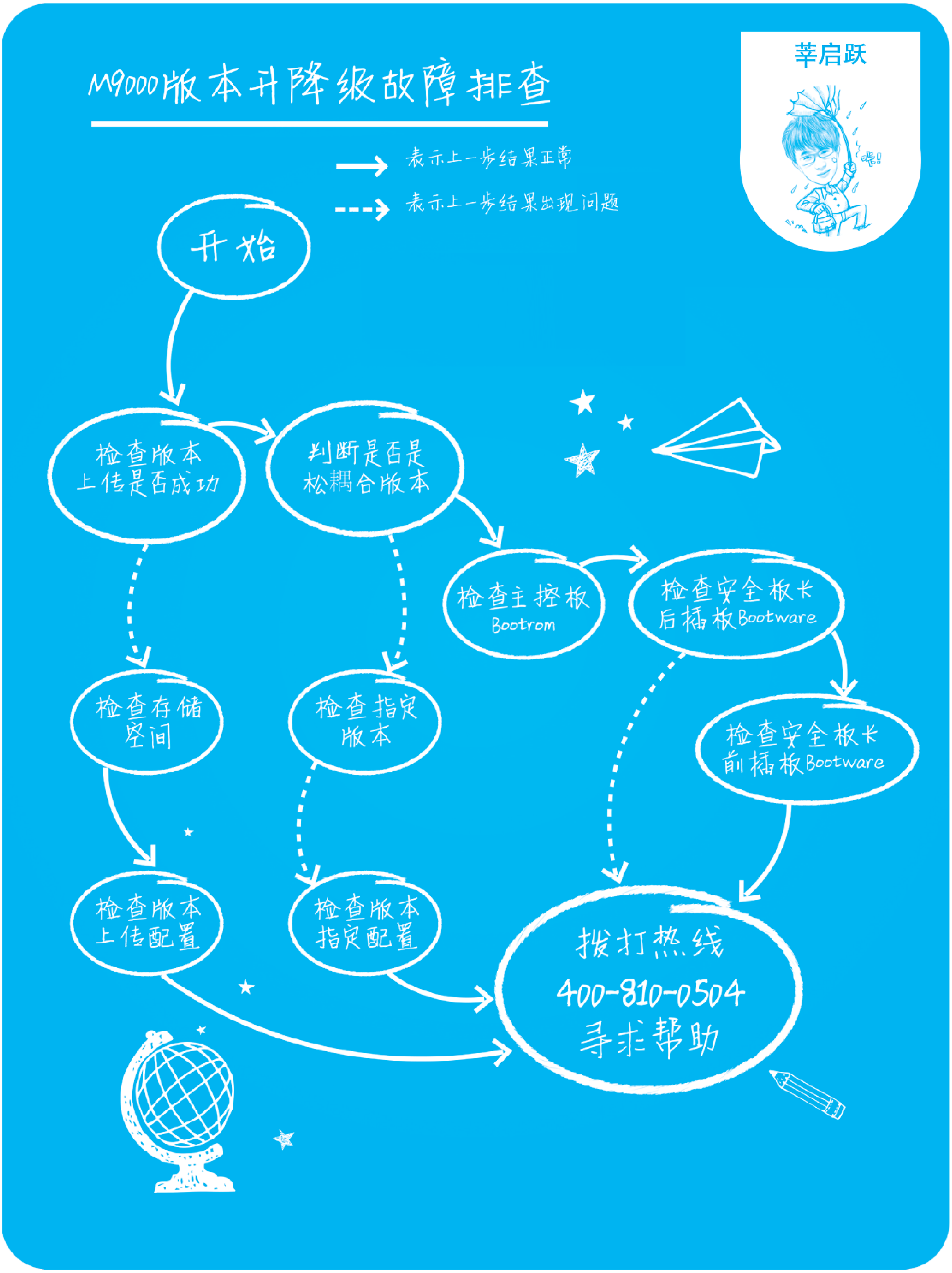
Summary Count :1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/0           Static  60   0          60.100.1.2      GE1/1/0/23

<H3C>display ip routing-table 172.31.0.1

Summary Count : 2

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/0           Static  60   0          60.100.1.2      GE1/1/0/23
172.31.0.0/24       Direct  0    0          192.168.100.2   GE1/1/0/1
```


M9000版本升降级故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
检查版本上传是否成功
判断是否是松耦合版本
检查主控板Bootrom
检查安全板卡后插板Bootware
检查安全板卡前插板Bootware
检查存储空间
检查指定版本
检查版本上传配置
检查版本指定配置
拨打热线
400-810-0504
寻求帮助

1．开始

M9000 分松耦合和紧耦合版本，采用松耦合版本时，安全业务板与 M9000 机框无统一管理关系，软件升级操作与 V5 平台机框、安全板卡各自独立升级管理方式相同；采用紧耦合版本时，防火墙等安全业务板与 M9000 机框为统一管理关系的软件版本。

M9000 版本升级故障的排查思路是：首先明确现网采用松耦合还是紧耦合，确认所需版本，包括 Bootrom 及软件版本，之后排查版本上传是否成功，最后检查版本升级相关配置是否正确。

2．流程图相关操作说明

（1）检查版本上传是否成功

① 通过 Bootware 方式上传。在设备加电启动时进入 Bootware 菜单，通过显示存储介质中所有文件来确认版本上传是否成功。

例如：在 Bootware 菜单下，确认文件 SECPATH9000M-CMW710-R9115P02.ipe 成功上传到 flash 下，且文件大小与官网版本一致，若 Bootware 菜单下未出现该文件，或者文件大小与官网版本不一致，则说明版本上传失败。

```
Enter < Storage Device Operation > to select device.

--------------------<EXTENDED-BOOTWARE MENU> --------------------
|<1> Boot System                                                |
|<2> Enter Serial SubMenu                                       |
|<3> Enter Ethernet SubMenu                                     |
|<4> File Control                                               |
|<5> Restore to Factory Default Configuration                   |
|<6> Skip Current System Configuration                          |
|<7> BootWare Operation Menu                                    |
|<8> Skip Authentication for Console Login                      |
|<9> Storage Device Operation                                   |
|<0> Reboot                                                     |
-----------------------------------------------------------------
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 4

----------------------------<File CONTROL> ----------------------------
|Note:the operating device is flash                             |
| <1> Display All File(s)                                       |
|<2> Set Image File type                                        |
|<3> Set Bin File type                                          |
|<4> Delete File                                                |
|<0> Exit To Main Menu                                          |
-----------------------------------------------------------------
Enter your choice(0-4): 1
```

```
Display all file(s) in flash:
 'M' = MAIN        'B' = BACKUP        'N/A' = NOT ASSIGNED
-------------------------------------------------------------------------------
|NO. Size(B)   Time                 Type   Name                              |
|1   2398      Feb/06/2015 03:55:42 N/A    flash:/pki/https-server.p12       |
|2   975       Feb/06/2015 03:55:42 N/A    flash:/pkey/dsa/keybbb.key        |
|3   1311      Feb/06/2015 03:55:42 N/A    flash:/pkey/rsa/keyaaa.key        |
|4   223       Feb/06/2015 03:55:42 N/A    flash:/pkey/ecdsa/keyccc.key      |
...
|37 99980288  Feb/09/2015 09:01:43 N/A    flash:/ SECPATH9000M-CMW710-R9115 |
| P02.ipe
...
```

② 通过命令行方式上传。在命令行下通过命令查看版本文件是否上传成功，以及文件大小是否正确。

命令：*pwd*

dir [*/all*] [*file-url* | */all-filesystems*]

例如：通过命令查看版本文件 SECPATH9000M-CMW710-R9115P02.ipe 成功上传到主用主控板 flash 下，且文件大小与官网版本一致。若 flash 下未出现该文件，或者文件大小与官网版本不一致，则说明版本上传失败。

```
<H3C>pwd
flash:
<H3C>dir
Directory of flash:
...
   3 -rw-      99980288 Feb 09 2015 09:13:06    SECPATH9000M-CMW710-R9115P02.ipe
   4 -rw-         10047 Dec 18 2014 05:04:55    startup.cfg
   5 -rw-        136331 Dec 18 2014 05:04:56    startup.mdb
...
```

(2) 检查存储空间

检查主控板 Flash、防火墙板 CF 卡当前剩余存储空间。当前主用主控板(准备执行升级操作的主控板)应预留 320MB 以上的空闲空间，非主用主控板应预留 160MB 以上的空闲空间，防火墙插卡应预留 60MB 以上的空闲空间。各个防火墙板都要检查，剩余空间不足会导致升级过程中系统无法向存储介质写入解压后的板卡文件，需要彻底删除无用文件以释放存储空间。

① 通过 Bootware 方式。例如：在 Bootware 菜单下，确认当前主控板 flash 可用空间为 1412KB。

```
------------------------ <EXTENDED-BOOTWARE MENU> ------------------------
|<1> Boot System                                                         |
|<2> Enter Serial SubMenu                                                |
|<3> Enter Ethernet SubMenu                                              |
|<4> File Control                                                        |
|<5> Restore to Factory Default Configuration                            |
|<6> Skip Current System Configuration                                   |
|<7> BootWare Operation Menu                                             |
|<8> Skip Authentication for Console Login                               |
```

```
| <9> Storage Device Operation                                          |
|<0> Reboot                                                             |
-------------------------------------------------------------------------
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 9

----------------------- <DEVICE CONTROL> --------------------------------
| <1> Display All Available Nonvolatile Storage Device(s)               |
|<2> Set The Operating Device                                           |
|<3> Set The Default Boot Device                                        |
|<0> Exit To Main Menu                                                  |
-------------------------------------------------------------------------
Enter your choice(0-3): 1

Display all available nonvolatile storage device(s):
-------------------------------------------------------------------------
|NO.  Device Name  File System  Total Size  Available Space             |
|1    flash        JFFS2        503808KB    1412KB                      |
-------------------------------------------------------------------------
```

② 通过命令行方式。除当前主用主控板外，切换至其他存储空间路径时需要写完整路径。

首先，通过命令切换至相应的存储介质。

命令：*cd* [*drive*:][/]*path*

例如：通过命令切换至防火墙业务板 CF 卡。

```
<H3C>display device
Chassis  Slot  Type           State    Subslot  Soft Ver         Patch Ver
1        0     NONE           Absent   0        NONE             None
1        1     NSQ1GP24TXEA0  Normal   0        M9010-9115P02    None
1        2     NONE           Absent   0        NONE             None
1        3     NONE           Absent   0        NONE             None
1        4     NSQ1SUPB0      Master   0        M9010-9115P02    None
1        5     NONE           Absent   0        NONE             None
1        6     NONE           Absent   0        NONE             None
1        7     NSQ1FWCEA0     Normal   0        M9010-9115P02    None
               CPU 1          Normal   0        M9010-9115P02
1        8     NONE           Absent   0        NONE             None
1        9     NONE           Absent   0        NONE             None
1        10    NSQ1FAB08D0    Normal   0        M9010-9115P02    None
1        11    NSQ1FAB08D0    Normal   0        M9010-9115P02    None
1        12    NSQ1FAB08D0    Normal   0        M9010-9115P02    None
1        13    NSQ1FAB08D0    Normal   0        M9010-9115P02    None
2        0     NONE           Absent   0        NONE             None
2        1     NSQ1GP24TXEA0  Normal   0        M9010-9115P02    None
2        2     NONE           Absent   0        NONE             None
2        3     NONE           Absent   0        NONE             None
2        4     NSQ1SUPB0      Standby  0        M9010-9115P02    None
2        5     NONE           Absent   0        NONE             None
2        6     NONE           Absentv  0        NONE             None
2        7     NSQ1FWCEA0     Normal   0        M9010-9115P02    None
               CPU 1          Normal   0        M9010-9115P02
```

```
2          8       NONE           Absent   0       NONE            None
2          9       NONE           Absent   0       NONE            None
2          10      NSQ1FAB08D0    Normal   0       M9010-9115P02   None
2          11      NSQ1FAB08D0    Normal   0       M9010-9115P02   None
2          12      NONE           Absent   0       NONE            None
2          13      NONE           Absent   0       NONE            None
<H3C>cd ?
  STRING                      [drive][path]
  chassis1#slot4#flash:       Device name
  chassis1#slot7.1#cfa0:      Device name
  chassis2#slot4#flash:       Device name
  chassis2#slot7.1#cfa0:      Device name
  flash:                      Device name
<H3C>cd chassis1#slot7.1#cfa0:/
<H3C>pwd
chassis1#slot7.1#cfa0:
```

然后，通过命令查看当前存储介质的可用空间是否满足需求。

命令：*dir*

例如：通过命令查看当前防火墙业务板 CF 卡可用空间为 159400KB，满足需求。

```
<H3C>dir
Directory of chassis1#slot7.1#cfa0:
   0 -rw-  4875264 Jan 04 2015 07:00:50   BLADE3FWM9000-CMW710-BOOT-E9114P05.bin
   1 -rw-  4971520 Feb 06 2015 03:46:50   BLADE3FWM9000-CMW710-BOOT-R9115P02.bin
   2 -rw-  42277888 Jan 04 2015 07:01:58  BLADE3FWM9000-CMW710-SYSTEM-E9114P05.bin
   3 -rw-  42763264 Feb 06 2015 03:47:56  BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin
   4 drw-         - Feb 02 2015 02:18:02   context
   5 drw-         - Nov 03 2014 02:12:40   diagfile
   6 -rw-      1956 Feb 06 2015 03:48:34   ifindex.dat
   7 -rw-         0 Nov 03 2014 02:12:42   lauth.dat
   8 drw-         - Nov 03 2014 02:12:40   logfile
   9 drw-         - Feb 09 2015 04:55:12   pkey
  10 drw-         - Feb 09 2015 04:55:11   pki
  11 drw-         - Nov 03 2014 02:12:40   seclog

252164 KB total (159400 KB free)
```

（3）检查版本上传配置

Bootware 和命令行下均可以通过 TFTP 和 FTP 两种方式上传文件，首先应确保设备与 FTP/TFTP 服务器之间路由可达，采用命令行 FTP 方式上传时，传输模式应该设置为二进制模式。

命令：*binary*

例如：设备通过 FTP 方式连接到 FTP 服务器 10.10.241.22，修改传输模式为 binary。

```
<H3C>ftp 10.10.241.22
Press CTRL+C to abort.
Connected to 10.10.241.22 (10.10.241.22).
220 3Com 3CDaemon FTP Server Version 2.0
User (10.10.241.22:(none)): admin
331 User name ok, need password
Password:
```

```
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Type set to I.
ftp>
```

（4）判断是否是松耦合版本

目前松耦合版本的使用场景为多插卡方案，即需要 IPS/ACG/LB/SSL VPN 等安全板卡。采用松耦合方案时，流量采用传统手工引流方式；采用紧耦合方案时，可采用自动分流方式。因此，需要根据现网需求确认版本是否为松耦合版本。

（5）检查指定版本

① 通过 Bootware 方式。例如：在 Bootware 菜单下，确认当前主控板的 MAIN 文件为 M9000-CMW710-SYSTEM-R9115P02.bin 和 M9000-CMW710-BOOT-R9115P02.bin。

```
Enter < Storage Device Operation > to select device.

------------------------ <EXTENDED-BOOTWARE MENU> ------------------------
|<1> Boot System                                                          |
|<2> Enter Serial SubMenu                                                 |
|<3> Enter Ethernet SubMenu                                               |
| <4> File Control                                                        |
|<5> Restore to Factory Default Configuration                             |
|<6> Skip Current System Configuration                                    |
|<7> BootWare Operation Menu                                              |
|<8> Skip Authentication for Console Login                                |
|<9> Storage Device Operation                                             |
|<0> Reboot                                                               |
---------------------------------------------------------------------------
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 4

----------------------------------- <File CONTROL> ------------------------
|Note:the operating device is flash                                       |
| <1> Display All File(s)                                                 |
|<2> Set Image File type                                                  |
|<3> Set Bin File type                                                    |
|<4> Delete File                                                          |
|<0> Exit To Main Menu                                                    |
---------------------------------------------------------------------------
Enter your choice(0-4): 1

Display all file(s) inflash:
'M' = MAIN        'B' = BACKUP        'N/A' = NOT ASSIGNED
---------------------------------------------------------------------------
|NO.  Size(B)   Time                  Type   Name                         |
|1    2398      Feb/06/2015 03:55:42 N/A    flash:/pki/https-server.p12  |
|2    975       Feb/06/2015 03:55:42 N/A    flash:/pkey/dsa/keybbb.key   |
|3    1311      Feb/06/2015 03:55:42 N/A    flash:/pkey/rsa/keyaaa.key   |
|4    223       Feb/06/2015 03:55:42 N/A    flash:/pkey/ecdsa/keyccc.key |
...
```

```
|31   90513408   Feb/09/2015 09:44:47 M        flash:/M9000-CMW710-SYSTEM-R9115        |
|P02.bin
|32   9459712    Feb/09/2015 09:41:43 M      flash:/ M9000-CMW710-BOOT-R9115P02        |
|.bin
…
```

② 通过命令行方式。在命令行下可以查看下次启动版本。

命令：*display boot-loader*

例如：通过命令查看主控板下次启动版本为 M9000-CMW710-BOOT-R9115P02.bin 及 M9000-CMW710-SYSTEM-R9115P02.bin，防火墙板下次启动版本为 BLADE3FWM9000-CMW710-BOOT-R9115P02.bin 及 BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin。

```
<H3C>display boot-loader
Software images on chassis 1 slot 4:
Current software images:
  flash:/M9000-CMW710-BOOT-R9115.bin
  flash:/M9000-CMW710-SYSTEM-R9115.bin
Main startup software images:
  flash:/M9000-CMW710-BOOT-R9115P02.bin
  flash:/M9000-CMW710-SYSTEM-R9115P02.bin
Backup startup software images:
  flash:/M9000-CMW710-BOOT-E9114P01.bin
  flash:/M9000-CMW710-SYSTEM-E9114P01.bin
Software images on chassis 1 slot 7.1:
Current software images:
  cfa0:/BLADE3FWM9000-CMW710-BOOT-R9115.bin
  cfa0:/BLADE3FWM9000-CMW710-SYSTEM-R9115.bin
Main startup software images:
  cfa0:/BLADE3FWM9000-CMW710-BOOT-R9115P02.bin
  cfa0:/BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin
Backup startup software images:
  None
…
```

（6）检查版本指定配置

主控板及防火墙板的版本根据需要指定，并且指定参数 all。

命令：*boot-loader file flash*:/[*sysname*] *all main*

例如：在命令行下指定主控板下次启动文件为 SECPATH9000M-CMW710-R9115P02.ipe，防火墙插卡下次启动文件为 SECBLADENGFW-CMW710-R9115P02.ipe。

```
<H3C>boot-loader file flash:/SECPATH9000M-CMW710-R9115P02.ipe all main
//指定主控板版本
Verifying the IPE file and the images.......Done.
H3C SecPath M9010 images in IPE:
  M9000-CMW710-BOOT-R9115P02.bin
  M9000-CMW710-SYSTEM-R9115P02.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to chassis 1 slot 4.
Decompressing file M9000-CMW710-BOOT-R9115P02. bin to flash:/M9000-CMW710-BOOT-R9115P02.bin..........Done.
Decompressing file M9000-CMW710-SYSTEM-R9115P02. bin to flash:/M9000-CMW710-SYSTEM-R9115P02.bin...............................................................................Done.
```

```
The images that have passed all examinations will be used as the main startup software images at the next reboot on chassis 1 slot 4.
Loading...%Dec 23 03:23:24:704 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 2 slot 4 is loading software images.
....%Dec 23 03:23:30:385 2014 H3C DEV/5/LOAD_FINISHED: Board in chassis 2 slot 4 has finished loading software images.
.........Done.
Loading.........%Dec 23 03:23:46:920 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 2 slot 4 is loading software images.
..........................%Dec 23 03:24:15:614 2014 H3C DEV/5/LOAD_FINISHED: Board in chassis 2 slot 4 has finished loading software images.
..........................................................................Done.
The images that have passed all examinations will be used as the main startup software images at the next reboot on chassis 2 slot 4.
Decompression completed.
Do you want to delete flash:/SECPATH9000M-CMW710-R9115P02.ipe now? [Y/N]:y
```

选择 Y 删除 IPE 文件，节省上传了版本文件的主用主控板 Flash 空间。

```
<H3C>boot-loader file flash:/SECBLADENGFW-CMW710-R9115P02.ipe all main
Verifying the IPE file and the images....Done.
Blade3fw-m9000 images in IPE:
  BLADE3FWM9000-CMW710-BOOT-R9115P02.bin
  BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to chassis 1 slot 4.
Decompressing file BLADE3FWM9000-CMW710-BOOT-R9115P02.bin to flash:/BLADE3FWM9000-CMW710-BOOT-R9115P02.bin.........Done.
Decompressing file BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin to flash:/BLADE3FWM9000-CMW710-SYSTEM-R9115P02.bin.................................................................................
Done.
Loading...%Dec 23 03:27:57:906 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 2 slot 7.1 is loading software images.
%Dec 23 03:27:57:906 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 1 slot 7.1 is loading software images.
%Dec 23 03:28:02:302 2014 H3C DEV/5/LOAD_FINISHED: Board in chassis 1 slot 7.1 has finished loading software images.
......Done.
Loading....%Dec 23 03:28:11:151 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 2 slot 7.1 is loading software images.
%Dec 23 03:28:11:151 2014 H3C DEV/4/BOARD_LOADING: Board in chassis 1 slot 7.1 is loading software images.
%Dec 23 03:28:26:245 2014 H3C DEV/5/LOAD_FINISHED: Board in chassis 1 slot 7.1 has finished loading software images.
.....................................Done.
The images that have passed all examinations will be used as the main startup software images at the next reboot on chassis 1 slot 7.1.
Specify the startup software image files for Blade3fw-m9000 to load from the parent device? [Y/N]:y
The images that have passed all examinations will be used as the load software image files for Blade3fw-m9000.
Decompression completed.
    Do you want to delete flash:/SECBLADENGFW-CMW710-R9115P02.ipe now? [Y/N]:y
```

(7) 检查主控板 Bootrom

主控板 SUPB 当前 Bootrom 版本应为 1.19。

在命令行下可以查看主控板 Bootrom 版本。

命令：*display version*

例如：通过命令查看主控板 Bootrom 版本为 119。

```
<H3C>display version
Uptime is 0 weeks,4 days,20 hours,5 minutes
H3C SecPath M9010 MPU(M) with 1 XLP316 Processor
BOARD TYPE:             NSQ1SUPB0
DRAM:                   8192M bytes
FLASH:                  500M bytes
NVRAM:                  512K bytes
PCB 1 Version:          VER.A
Bootrom Version:        119
CPLD 1 Version:         003
CPLD 2 Version:         003
CPLD 3 Version:         003
Release Version:        H3C SecPath M9010-9115
```

(8) 检查安全板卡后插板 Bootware

M9000 机框插二代安全业务板时，只能使用松耦合方式，需要修改安全板卡的后插板 Bootware 至 v5.01，涉及的插卡型号为 LSQ2FWBSC0/LSQ1ACGASC0/LSQ1IPSSC0/LSQ1SSLSC0/LSQ1LBSC0/LSQ1NSMSC0。

可以将 console 线连至安全板卡后插板串口查看当前后插板 Bootware 版本，图 6-125 所示为升级正确后的后插板 Bootware 界面。

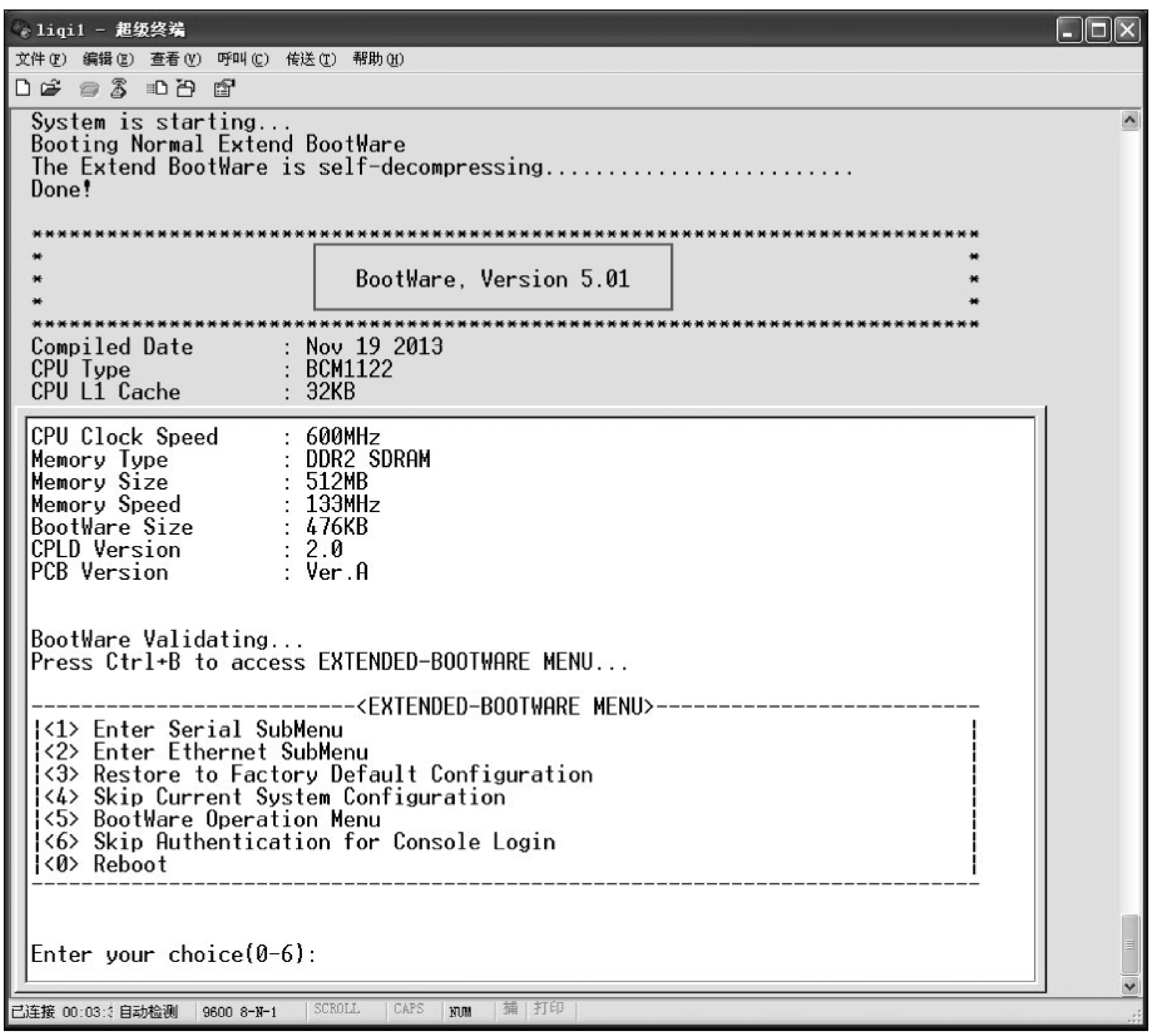


图 6-125　升级后的后插板 Bootware 界面

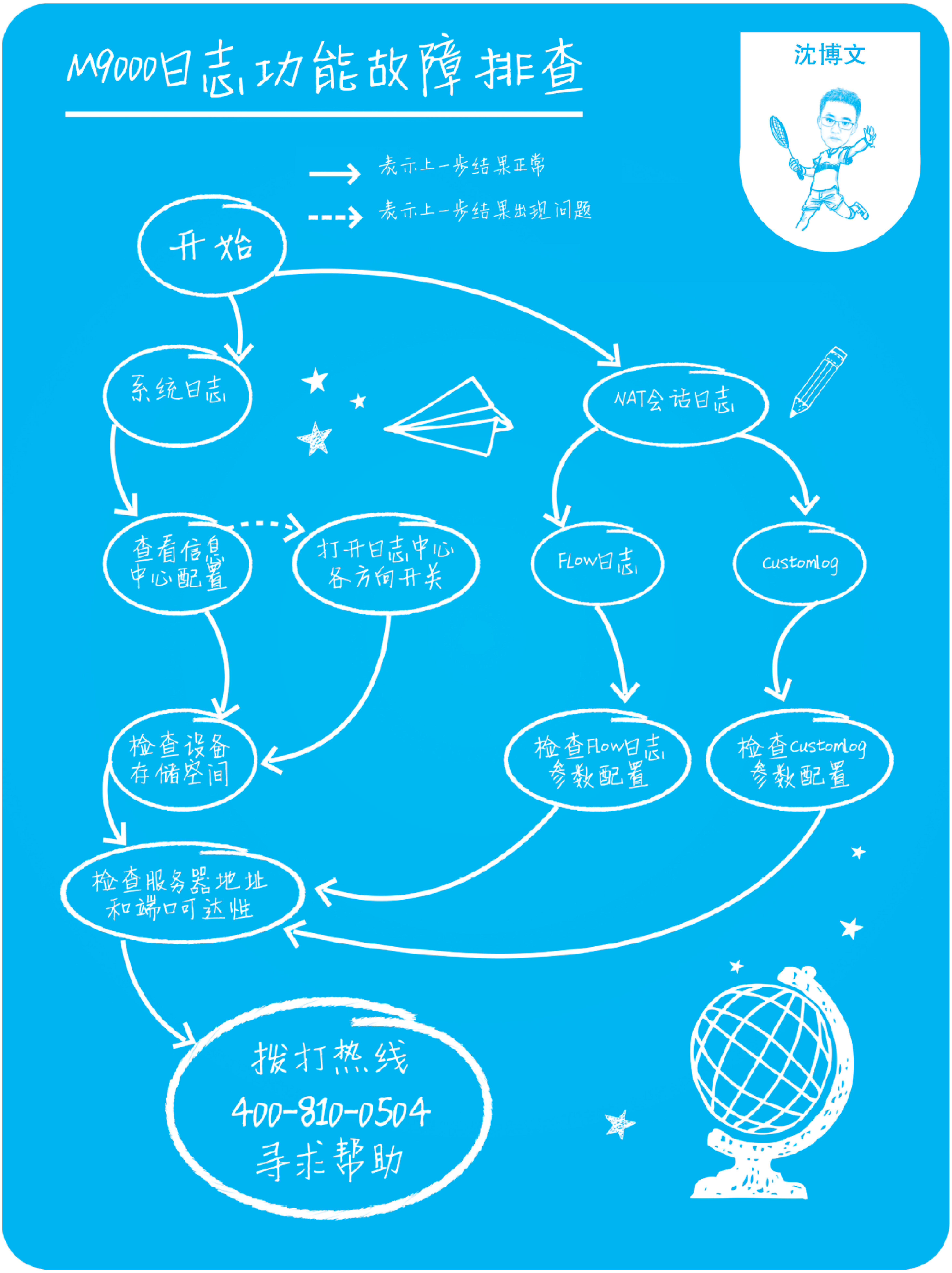
(9) 检查安全板卡前插板 Bootware

M9000 机框插三代安全业务板松耦合时，需要修改安全板卡的前插板 Bootware 至 v1.20，涉及的插卡型号为：LSU1IPSBEA0/NSQ1FWCEA0。

例如：可以在设备启动时查看当前 IPS 安全板卡的前插板 Bootware 版本。

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU
Press Ctrl+T to start heavy memory test
Booting Normal Extend BootWare........
The Extend BootWare is self-decompressing......Done!

*************************************************************************************
*                                                                                   *
*                     H3C SecBlade IPS BootWare, Version 1.20                       *
*                                                                                   *
*************************************************************************************
Compiled Date         : Nov 20 2013
CPU Type              : XLP432
CPU Clock Speed       : 1500MHz
Memory Type           : DDR3 SDRAM
Memory Size           : 4096MB
Memory Speed          : 1333MHz
BootWare Size         : 768KB
Flash Size            : 8MB
cfa0 Size             : 999MB
CPLD_A Version        : 2.0
CPLD_B Version        : 1.0
CPLD_C Version        : 1.0
PCB Version           : Ver.A
```


M9000日志功能故障排查
沈博文
表示上一步结果正常
表示上一步结果出现问题
开始
系统日志
NAT会话日志
查看信息中心配置
打开日志中心各方向开关
Flow日志
customlog
检查设备存储空间
检查Flow日志参数配置
检查customlog参数配置
检查服务器地址和端口可达性
拨打热线
400-810-0504
寻求帮助

1. 开始

日志功能是 M9000 的信息枢纽，包括系统日志和 NAT 日志两种。系统日志能够对系统内所有模块的日志信息进行分类、管理，为网络管理员监控网络运行情况和诊断网络故障提供有力的支持；NAT 日志是为满足网络管理员做安全审计的需要，对用户的访问信息、用户 IP 地址的转换信息、用户的网络流量信息等进行记录的一种日志类型，可以通过一定的格式发给日志主机。

M9000 日志功能问题排查的主要思路是：首先根据不同的日志类型确认排查思路；系统日志输出要保证信息中心开关处于打开状态，明确需要排查信息中心哪个方向的故障，确认每个输出方向配置是否有问题；会话日志的故障排查也分为两种，明确需要发送二进制形式的会话日志还是十进制形式的会话日志，然后分别确认配置是否存在问题；无论何种日志的输出，只要需要发送到日志服务器，那么就需要确保日志服务器的 IP 地址和端口号可达。

2. 流程图相关操作说明

(1) 查看信息中心配置

默认情况下，M9000 信息中心开关处于开启状态，并且可以将相应等级的日志信息输出到控制台、监控终端、Logbuffer 以及 logfile 文件内；如果信息中心开关处于关闭状态，那么信息中心的所有功能皆不可用，所以第一步需要查看信息中心的配置。

命令：*display info-center*

info-center enable

```
[H3C] display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    1.1.1.1,
    port number: 514, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512
    Current messages 512, dropped messages 0, overwritten messages 337
Log file: Enabled
Security log file: Disabled
Information timestamp format:
    Log host: Date
    Other output destination: Date

[H3C]info-center enable
Information center is enabled.
```

(2) 打开日志中心各方向开关

M9000 信息中心，可以通过配置将日志信息输出到控制台、监控终端、Loghost、Logbuffer 以及 logfile 文件内，通过查看信息中心配置可以确认信息中心各个输出方向开关是否打开，如果没有打开，可以通过命令打开。

命令：*display info-center*
terminal monitor
info-center enable
info-center logbuffer
info-center loghost x.x.x.x port xxx

```
[H3C] display info-center
Information Center:Enabled
Console: Enabled
Monitor: Enabled
Log host:Enabled
    1.1.1.1,
    port number: 514, host facility: local7
Log buffer:Enabled
    Max buffer size 1024, current buffer size 512
    Current messages 512, dropped messages 0, overwritten messages 337
Log file:Enabled
Security log file: Disabled
Information timestamp format:
    Log host: Date
    Other output destination: Date

<H3C>terminal monitor
The current terminal is enabled to display logs.

[H3C]info-center enable
Information center is enabled.

[H3C]info-center logbuffer

[H3C]info-center loghost 1.1.1.1 port 514 facility local7
```

（3）检查设备存储空间

如果需要将日志输出到 Logfile，那么需要确保设备存储空间至少要有 10MB 空间剩余。

命令：*dir*

```
<H3C>dir
Directory of flash:
   0  -rw-      10125 Sep 11 2014 01:46:04   Bak_20140911.cfg
   1  -rw-    9268224 Nov 03 2014 01:14:23   M9000-CMW710-BOOT-E9114P05.bin
   2  -rw-   89675776 Nov 03 2014 01:15:43   M9000-CMW710-SYSTEM-E9114P05.bin
   3  -rw-   47160320 Nov 03 2014 01:12:30   SECBLADENGFW-CMW710-E9114P05.ipe
   4  -rw-   98951168 Nov 03 2014 01:05:59   SECPATH9000M-CMW710-E9114P05.ipe
   5  drw-          - Apr 21 2014 17:42:34   diagfile
   6  -rw-       1806 Nov 26 2014 00:39:41   ifindex.dat
   7  -rw-          0 Jul 28 2014 14:50:08   lauth.dat
   8  drw-          - Jan 12 2014 22:17:24   license
   9  drw-          - Nov 26 2014 07:23:32   logfile
  10  drw-          - Nov 19 2014 01:41:56   pki
  11  drw-          - Jan 12 2014 22:17:24   seclog
  12  -rw-       8694 Nov 26 2014 00:39:41   startup.cfg
  13  -rw-     130152 Nov 26 2014 00:39:41   startup.mdb
  14  drw-          - Jun 25 2014 17:34:34   versionInfo

503808 KB total (92512 KB free)
```

（4）检查服务器地址和端口可达性

如果需要将日志发送到日志服务器，那么需要保证日志服务器地址可达，并且相应的端口在日志服务器已打开，可以通过 ping 等手段确认。如果服务器不可达，需要检查 M9000 与服务器之间网络是否存在问题；如果服务器可以收到 M9000 发送的日志报文，但是无法解析到，需要确认日志服务器是否监听了防火墙发送日志的端口。

命令：*ping x.x.x.x*

```
<H3C>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=255 time=0.536 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=255 time=0.435 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=255 time=6.886 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=255 time=0.416 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=255 time=0.424 ms

--- Ping statistics for 1.1.1.1 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.416/1.739/6.886/2.574 ms
<H3C>%Nov 27 09:45:33:548 2014 H3C PING/6/PING_STATISTICS: Ping statistics for 1.1.1.
1: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev =
0.416/1.739/6.886/2.574 ms.
```

（5）FLow 日志

设备根据报文的五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议号）对用户访问网络的流进行分类统计，并生成用户流（Flow）日志。Flow 日志目前主要用来记录用户访问网络所产生的 NAT 会话相关信息，包括五元组和发送、接收的字节数等；网络管理员利用这些信息可以实时跟踪、记录、分析用户访问网络的情况。Flow 日志可以封装成二进制格式的 UDP 报文直接发送到日志主机，虽然 Flow 也支持输出到信息中心转换为十进制输出，但是传输效率低，并对会对设备性能产生重大影响，严禁 Flow 日志输出到信息中心。

（6）检查 Flow 日志参数配置

在配置 Flow 日志前需要通过 nat log enable 命令使能 NAT 日志功能，并根据用户需求选择开启 NAT 新建、删除会话日志和活跃流日志功能；然后确认配置了 userlog 发送 NAT 会话日志。

命令：*display userlog export*

display nat log

```
<H3C>display userlog export
Flow:
  Export flow log as UDP Packet.
  Version: 1.0
  Source ipv4 address:
  Source ipv6 address:
  Log load balance function: Disabled
  Local time stamp: Disabled
  Log host numbers: 1

Log host 1:
    Host/Port: 1.1.1.1/12345
```

```
        Total logs/UDP packets exported: 0/0

<H3C>display nat log
NAT logging:
  Log enable              : Enabled
  Flow-begin              : Disabled
  Flow-end                : Enabled
  Flow-active             : Disabled
  Port-block-assign       : Disabled
  Port-block-withdraw     : Disabled
  Alarm                   : Disabled
```

(7) Customlog

Customlog 类型的 NAT 会话日志是 M9000 针对国内三家运营商进行定制的 NAT 会话日志，根据不通运营商的要求开发的不通格式的十进制格式日志，如果需要在 M9000 上发送十进制 NAT 会话日志，必须采用 Customlog 类型的 NAT 会话日志。

(8) 检查 Customlog 参数配置

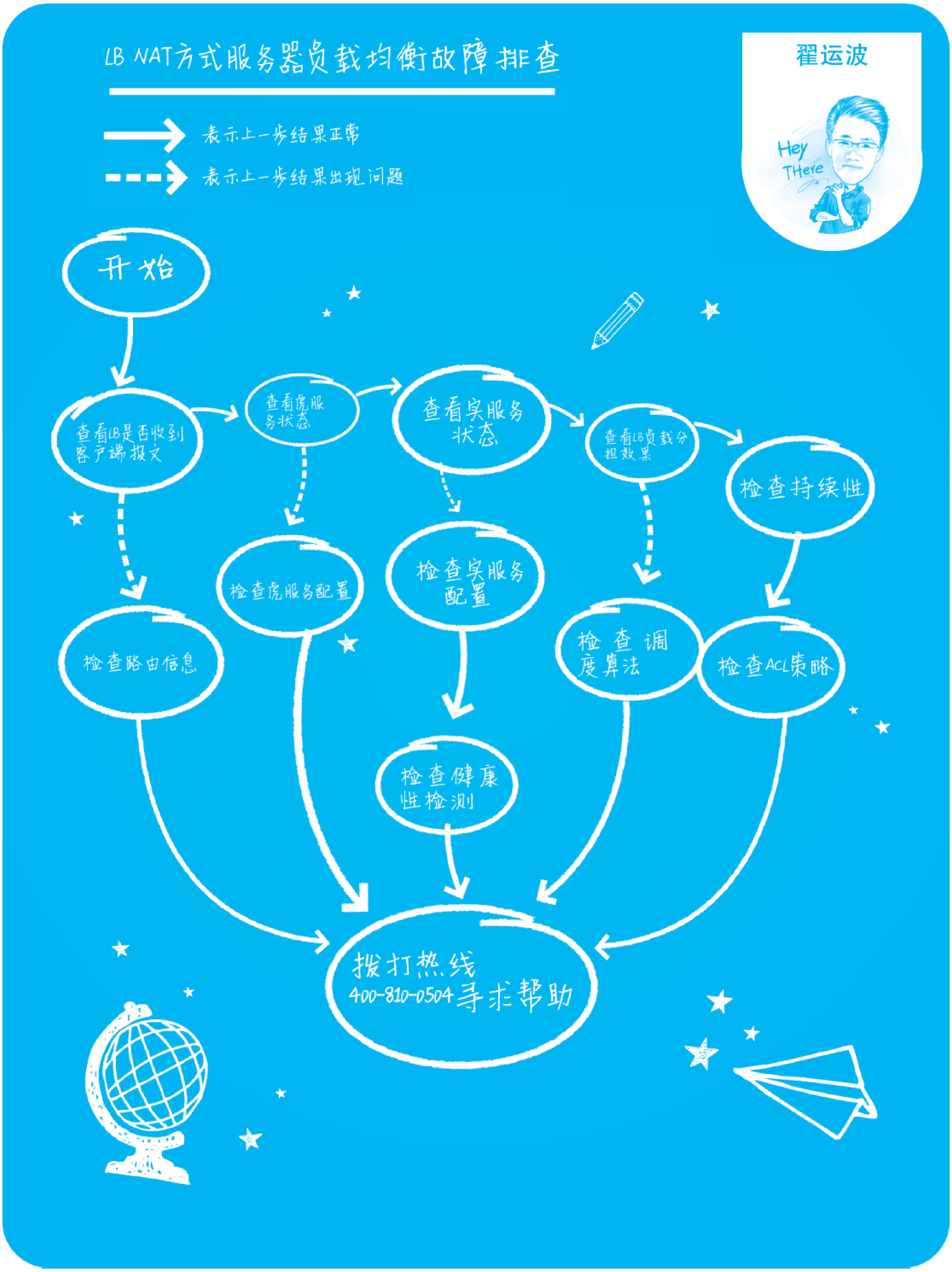
在配置 Customlog 日志前需要通过 nat log enable 命令使能 NAT 日志功能，并根据用户需求选择开启 NAT 新建、删除会话日志和活跃流日志功能；然后确认配置了 customlog 发送 NAT 会话日志。

命令：*display userlog export*

display current-configuration | *include customlog*

```
<H3C>display current-configuration | include customlog
 customlog format cmcc
 customlog host 1.1.1.1 port 12345 export cmcc-sessionlog cmcc-userlog

<H3C>display nat log
NAT logging:
  Log enable              : Enabled
  Flow-begin              : Disabled
  Flow-end                : Enabled
  Flow-active             : Disabled
  Port-block-assign       : Disabled
  Port-block-withdraw     : Disabled
  Alarm                   : Disabled
```


LB NAT方式服务器负载均衡故障排查
翟运波
Hey There
表示上一步结果正常
表示上一步结果出现问题
开始
查看LB是否收到客户端报文
查看虚服务状态
查看实服务状态
查看LB负载分担效果
检查持续性
检查路由信息
检查虚服务配置
检查实服务配置
检查调度算法
检查ACL策略
检查健康性检测
拨打热线
400-810-0504寻求帮助

06 安全产品 > 6.3 LB > 6.3.1 LB NAT 方式服务器负载均衡故障排查 > 步骤详解

1. 开始

服务器负载均衡技术可以将大量用户的业务分担给多台服务器，提高了业务的整体处理能力，同时保证了业务的高可靠性，NAT 方式是最常见的服务器负载均衡技术。NAT 方式服务器负载定位故障的思路是：先确认 LB 是否收到客户请求报文，然后检查虚服务和实服务状态，再检查调度算法，最后检查持续性和 ACL 策略。

2. 流程图相关操作说明

(1) 查看 LB 是否收到客户端报文

LB 将不同客户的请求分发给不同的服务器，从而实现负载分担的目的，所以定位问题时首先要判断 LB 是否收到客户端的请求报文，具体可以通过在 LB 上查看会话或者抓包的方法进行确认。

命令：*display session table source-ip x.x.x.x destination-ip y.y.y.y verbose*

例如：通过命令可以发现 LB 已经收到客户端 10.0.0.1 发来的请求报文。

```
[H3C]display session table source-ip 10.0.0.1 destination-ip 60.191.99.142 verbose
Initiator:
  Source IP/Port : 10.0.0.1/60931
  Dest IP/Port   : 60.191.99.142/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 192.168.1.2/80
  Dest IP/Port   : 10.0.0.1/60931
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP            State: TCP-EST
Start time: 2013-04-26 13:35:52   TTL: 3595s
Root                          Zone(in):
                              Zone(out):
Received packet(s)(Init): 2 packet(s) 92 byte(s)
Received packet(s)(Reply): 1 packet(s) 44 byte(s)
```

(2) 检查路由信息

如果通过查看会话或者抓包发现 LB 没有收到客户的请求报文，那么需要对路由进行排查，确保上行设备都有到达 LB 的虚服务 IP 地址的路由。

命令：*display ip routing-table x.x.x.x*

例如：LB 的虚地址是 60.191.99.142，通过命令看到上行设备已经有到 60.191.99.142 的路由。

```
<SW>display ip routing-table
Routing Tables: Public
         Destinations : 9          Routes : 9

Destination/Mask    Proto   Pre  Cost        NextHop         Interface

10.0.0.0/24         Direct  0    0           10.0.0.254      Vlan10
10.0.0.254/32       Direct  0    0           127.0.0.1       InLoop0
```

```
20.0.0.0/24        Direct 0     0          20.0.0.1        Vlan20
20.0.0.1/32        Direct 0     0          127.0.0.1       InLoop0
60.191.99.142/32   Static  60   0          20.0.0.2        Vlan20
...
```

另外，加入LB的虚服务IP地址和接口地址在同一物理网段，由于LB的虚地址目前不会响应ARP，所以需要在上行设备配置32位主机路由，或者将LB虚地址配置成接口sub地址或VRRP虚地址。

例如：LB的接口地址为20.0.0.0/24，虚服务IP地址是20.0.0.100，可以将虚服务地址配置成接口sub地址或者VRRP虚地址。

```
[H3C]display current-configuration interface Ten-GigabitEthernet 0/0.20
#
interface Ten-GigabitEthernet0/0.20
 vlan-type dot1q vid 20
 ip address 20.0.0.2 255.255.255.0
 ip address 20.0.0.100 255.255.255.0 sub
#
[H3C]display current-configuration interface Ten-GigabitEthernet 0/0.20
#
interface Ten-GigabitEthernet0/0.20
 vlan-type dot1q vid 20
 ip address 20.0.0.2 255.255.255.0
 vrrp vrid 20 virtual-ip 20.0.0.100
 vrrp vrid 20 priority 120
#
```

(3) 查看虚服务状态

登录到LB设备的Web管理界面，查看LB虚服务的状态是否正常，如果虚服务没有使能或者虚服务对应的所有实服务都出现异常，则虚服务会显示红灯，LB不会对命中虚服务的报文进行转发，所以一定要检查配置，确认虚服务已经使能，且状态显示为绿灯。

例如：进入LB的Web管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4协议"，单击"虚服务"页签，如图6-126所示，可以看到当前LB上http_service的虚服务状态正常，但是dns_service这个虚服务的状态不正常。

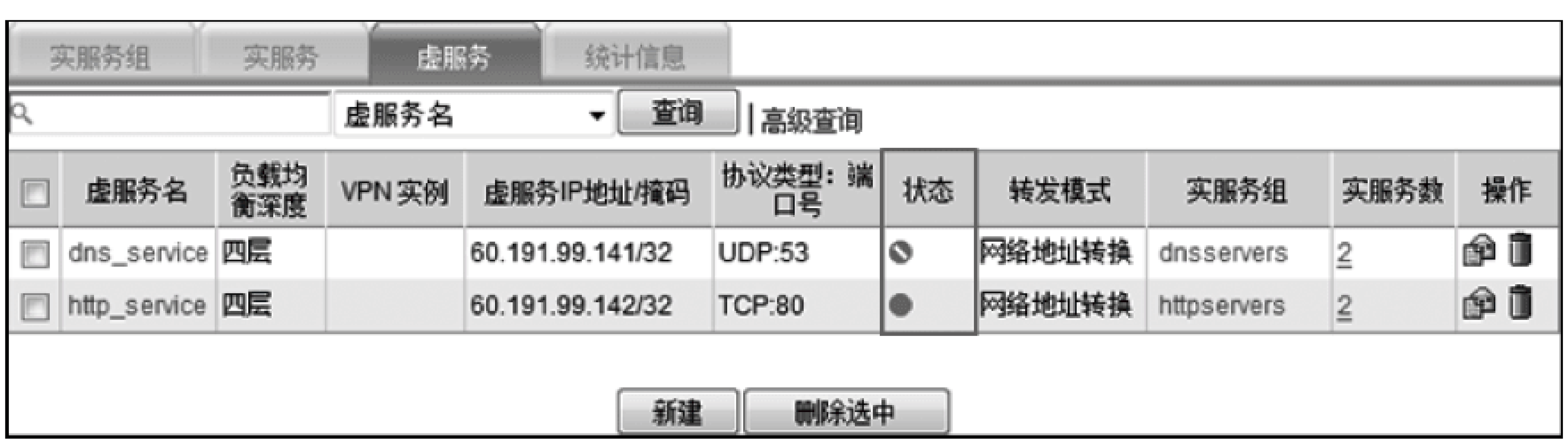


图6-126 虚服务

(4) 检查虚服务配置

如果虚服务的状态不正常，请仔细检查虚服务是否已经使能，然后检查虚服务的IP地址、掩码、协议和端口是否配置正确。

例如：进入LB的Web管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→

"IPv4 协议"，先单击"虚服务"页签，然后再单击对应虚服务后面的编辑按钮进入虚服务的配置界面，如图 6-127 和图 6-128 所示可以看到 http_service 这个虚服务的 IP 地址、掩码、协议及端口信息配置正确，并确认虚服务状态已经使能。



图 6-127 虚服务配置



图 6-128 修改虚服务

（5）查看实服务状态

LB 通过健康性检测实时监控各实服务的状态，状态正常的实服务显示绿灯，一旦检测到实服务故障，就显示红灯。LB 不会向故障的实服务分发流量，在日常维护过程中要及时关注实服务的状态。

例如：进入 LB 的 Web 管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4 协议"，单击"实服务"页签，如图 6-129 所示，可以看到 httpserver1 和 httpserver2 的健康性检测状态正常，dnsserver1 和 dnsserver2 的状态不正常。

（6）检查实服务配置

如果实服务的状态不正常，需要检查实服务的 IP 地址、端口以及健康性检测类型等配置。

例如：进入 LB 的 Web 管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4 协议"，先单击"实服务"页签，然后再单击对应实服务后面的编辑按钮进入实服务的配置界面，如图 6-130 和图 6-131 所示，看到实服务 httpserver1 的 IP 地址、端口配置正确，健康性检测方法和实服务组一致。

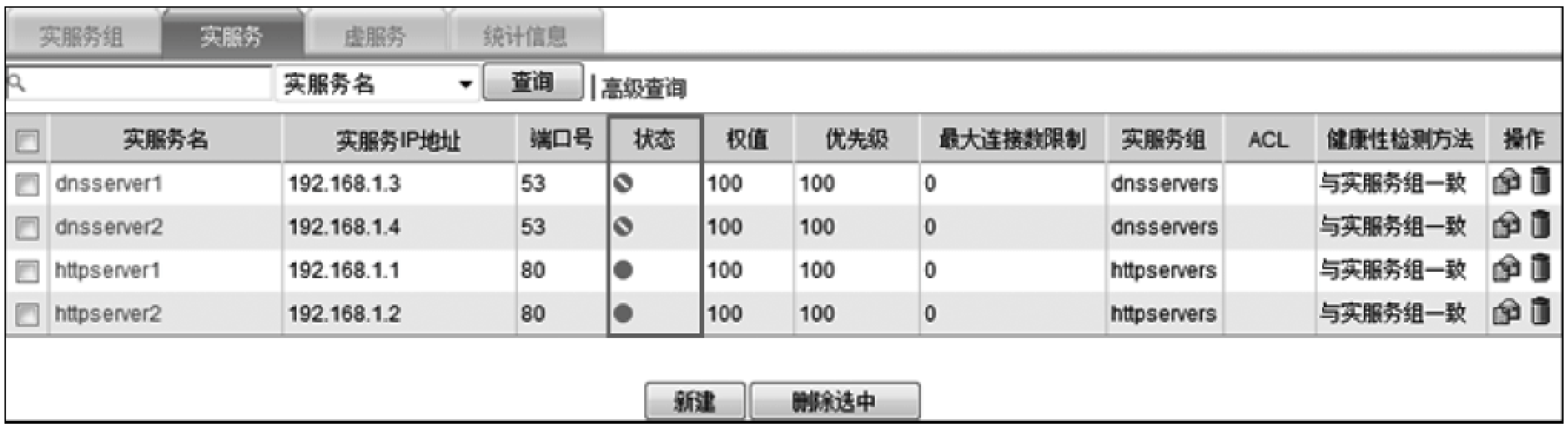


图 6-129　实服务



图 6-130　实服务配置

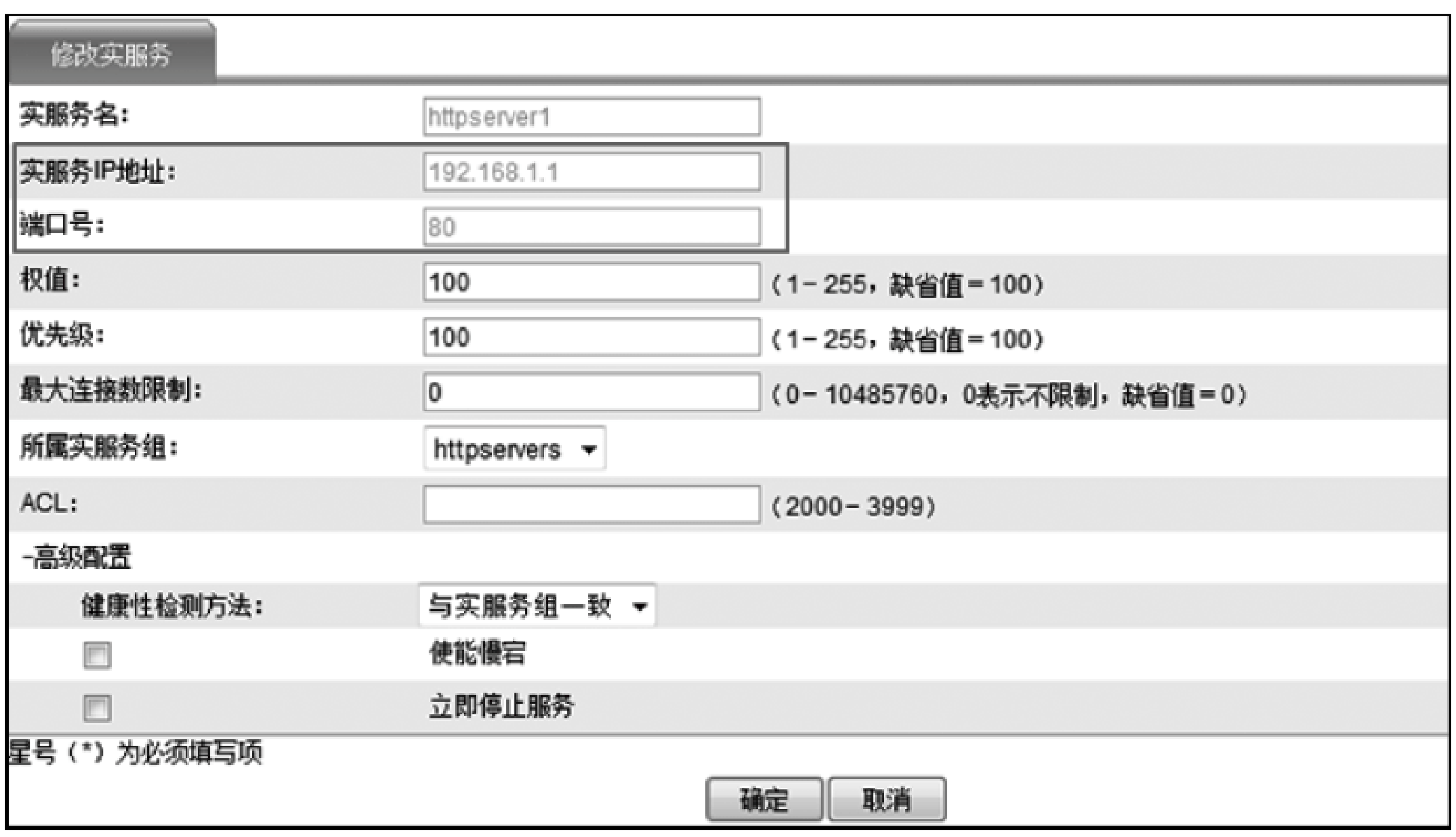


图 6-131　修改实服务

(7) 检查健康性检测

LB 通过健康性检测实时监控实服务的状态，如果实服务出现异常就显示红灯，并且会输出日志提示，当实服务出现异常的时候除了检查实服务的 IP 地址、端口等配置是否正确外，还应该及时根据实服务的健康性检测类型检查实服务的路由可达性、实服务提供业务的端口、进程或者应用程序是否正常。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“实服务”页签，然后再单击对应实服务后面的编辑按钮进入实服务的配置界面，看到 httpserver1 这个实服务的健康性检查选择的类型和实服务组一致，再单击“实服务组”页签，查看实服务组的健康性检测类型是 ICMP，然后进入 LB 的健康性检测配置页面检查

ICMP 的相关配置参数过程如图 6-132～图 6-134 所示。ICMP 主要用于检测服务的可达性，通过命令可以看到 LB 到实服务 192.168.1.1 的路由正常。



图 6-132 修改实服务

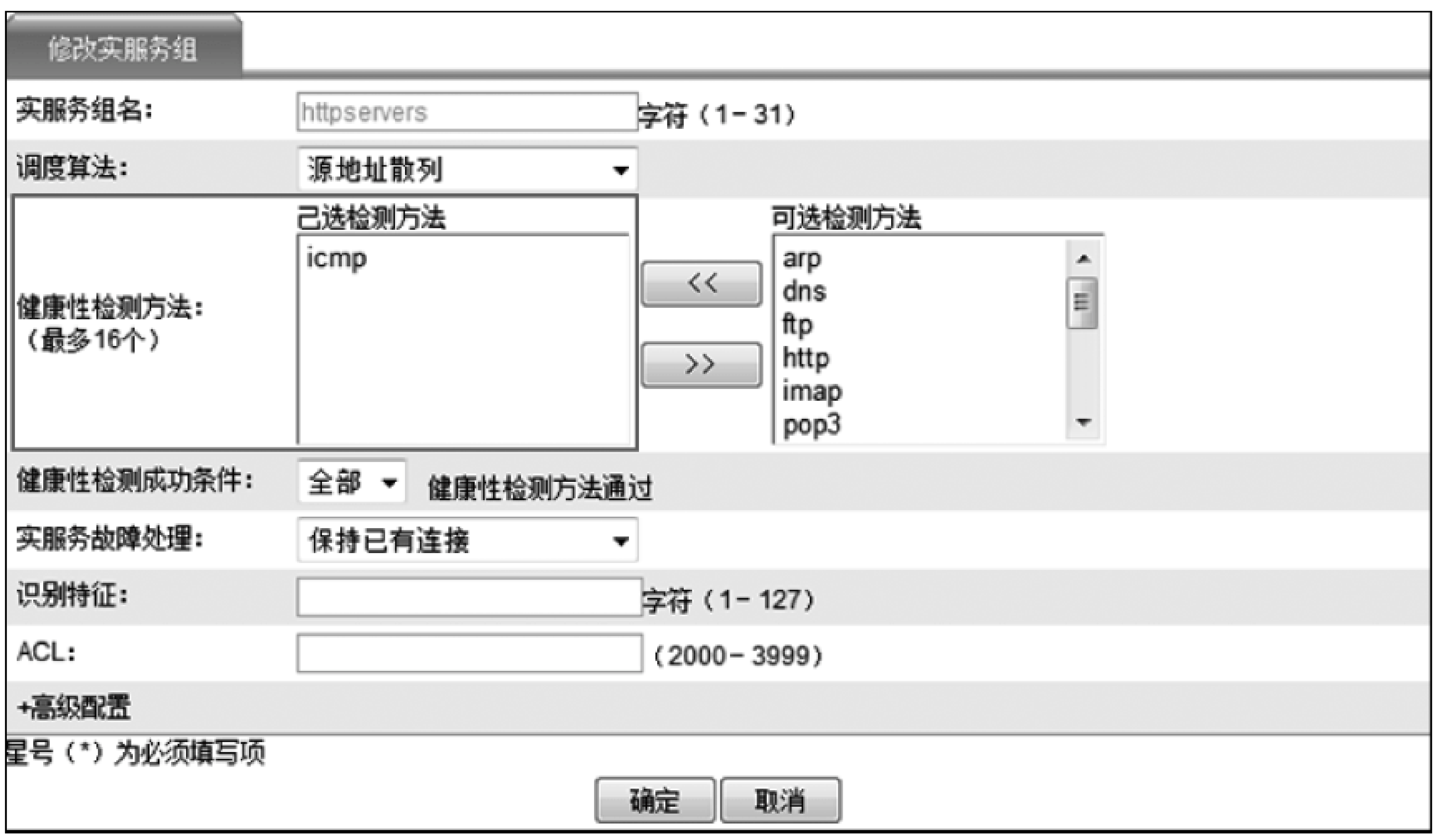


图 6-133 修改实服务组



图 6-134 修改健康性检测

```
<LB>display ip routing-table 192.168.1.1
Routing Table : Public
Summary Count : 1
Destination/Mask      Proto   Pre   Cost          NextHop          Interface
192.168.1.0/24        Direct  0     0             192.168.1.254    XGE0/0.50

<LB>ping 192.168.1.1
  PING 192.168.1.1: 56   data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=0 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

（8）查看 LB 负载分担效果

LB 提供了丰富的统计功能，可以对每个虚服务、实服务的连接数、连接速率、收发报文数等信息进行统计，通过统计信息可以看到 LB 当前的负载分担效果。

例如：进入 LB 的 Web 管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4 协议"，单击"统计信息"页签，如图 6-135 所示，可以查看虚服务 http_service 及其关联实服务 httpserver1 和 httpserver2 的总连接数、连接速率等信息，从当前统计情况来看，httpserver1 和 httpserver2 的负载效果非常均匀。

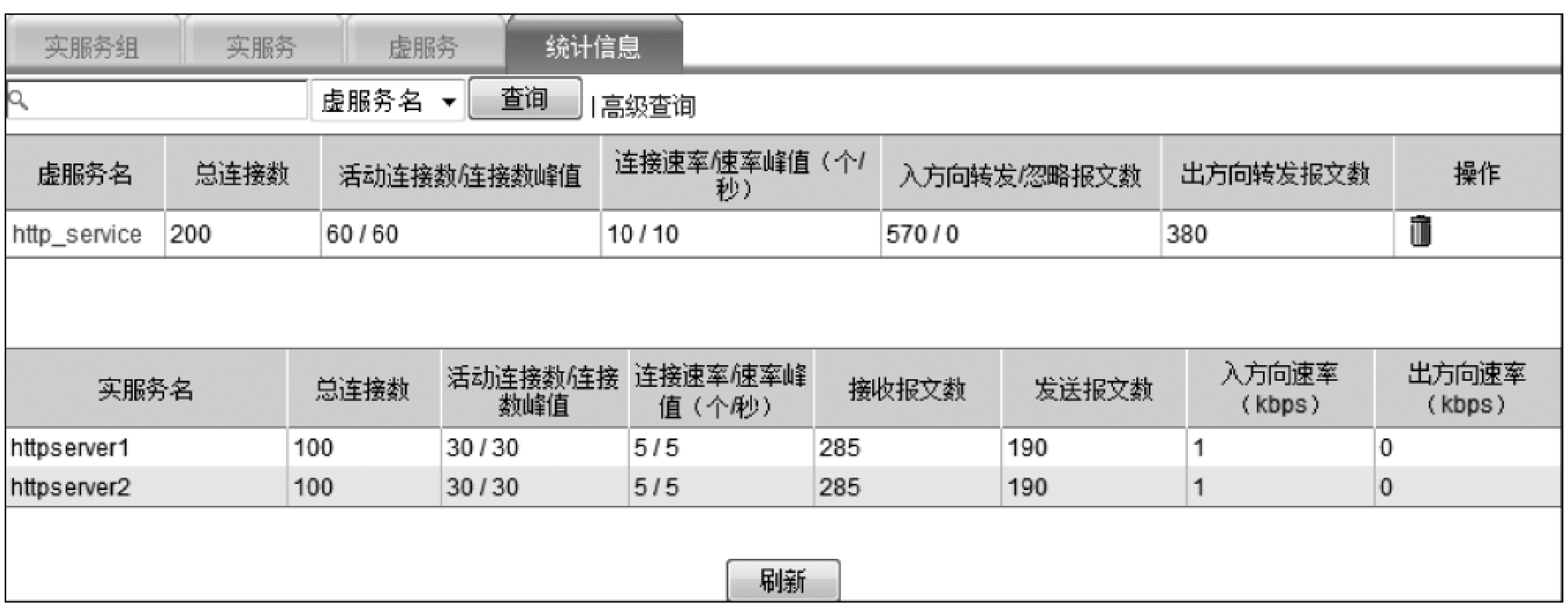


图 6-135　统计信息

（9）检查调度算法

如果通过虚服务的统计信息看到服务器负载的效果不均匀，应该及时根据业务情况调整调度算法。调整的时候先找到对应的虚服务，然后查看虚服务关联的是服务组，修改该实服务组的调度算法。

例如：进入 LB 的 Web 管理界面，在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4 协议"，先单击"虚服务"页签，查看 http_service 关联的实服务组是 httpservers，如图 6-136 所示，然后进入 httpservers 实服务组的配置界面调整其调度算法，如图 6-137 所示。



图 6-136 虚服务关联的实服务组



图 6-137 修改实服务组

（10）检查持续性

持续性就是在一定时间内将多个具有相同特性或者相关特性的连接持续发送到同一个服务器，LB 支持基于源 IP、源端口、目的 IP、目的端口等多方式的持续性，使能持续性功能后会，LB 会生成一张持续性表项，排错问题的时候先检查持续性表项是否正确，如果不正确需要及时调整持续性配置，另外可以通过会话查看报文的分发效果。

命令：*display load-balance persistence server vd-name root virtual-service xxxx*

display session table source-ipx.x.x.x destination-ip y.y.y.y verbose

例如：通过命令可以看到 LB 已经生产基于源 IP 的持续性表项，源 IP 是 10.0.0.1，对应的实服务是 192.168.1.2，表项的老化时间是 600 秒；另外通过会话可以看到来着 10.0.0.1 的报文被分发到 192.168.1.2 这台服务器。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]_h
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]display load-balance persistence server vd-name root virtual-service http_service
 Persistence method : Source-IP binding
```

```
Source-IP              Real-Server IP       Conn-Num          Age
 10.0.0.1               192.168.1.2           49               600
[H3C-hidecmd]quit

[H3C]display session table source-ip 10.0.0.1 destination-ip 60.191.99.142 verbose
Initiator:
  Source IP/Port : 10.0.0.1/50927
  Dest IP/Port   : 60.191.99.142/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 192.168.1.2/80
  Dest IP/Port   : 10.0.0.1/50927
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP              State: FIN-CLOSE
Start time: 2013-04-27 06:32:54   TTL: 0s
Root                          Zone(in):
                              Zone(out):
Received packet(s)(Init): 4 packet(s) 172 byte(s)
Received packet(s)(Reply): 4 packet(s) 907 byte(s)
```

如果持续性表项无法生成或者不正确，请登录到 LB 的 Web 管理界面检查持续性的配置是否正确。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“虚服务”页签，然后再单击 http_service 虚服务后面的编辑按钮进入虚服务配置界面，如图 6-138 所示，可以看到持续性选择了“源地址方式”，持续性表项生命值是 600 秒。



图 6-138　虚服务配置

（11）检查 ACL 策略

在某些应用场景下，客户要求将某些特点的数据流分发给特定的服务器，在 LB 上可以通

过 ACL 策略来实现，在排查的过程中可以通过会话来查看 ACL 策略是否生效，如果不生效需要仔细检查 ACL 策略的配置。

命令：*display acl xxxx*

display session table source-ipx.x.x.x destination-ip y.y.y.y verbose

例如：客户要求将来自 10.0.0.10 的所有流量分发给 192.168.1.1 这台实服务，命令行下面创建了一个 ACL 3001，定义需要转发的流量，然后在 LB WEB 管理界面将 ACL 3001 关联到 192.168.1.1 这台实服务，如图 6-139 所示。

```
[H3C]display acl 3001
Advanced ACL  3001, named -none-, 1 rule,
ACL's step is 5
 rule 0 permit ip source 10.0.0.10 0 (24 times matched)
```

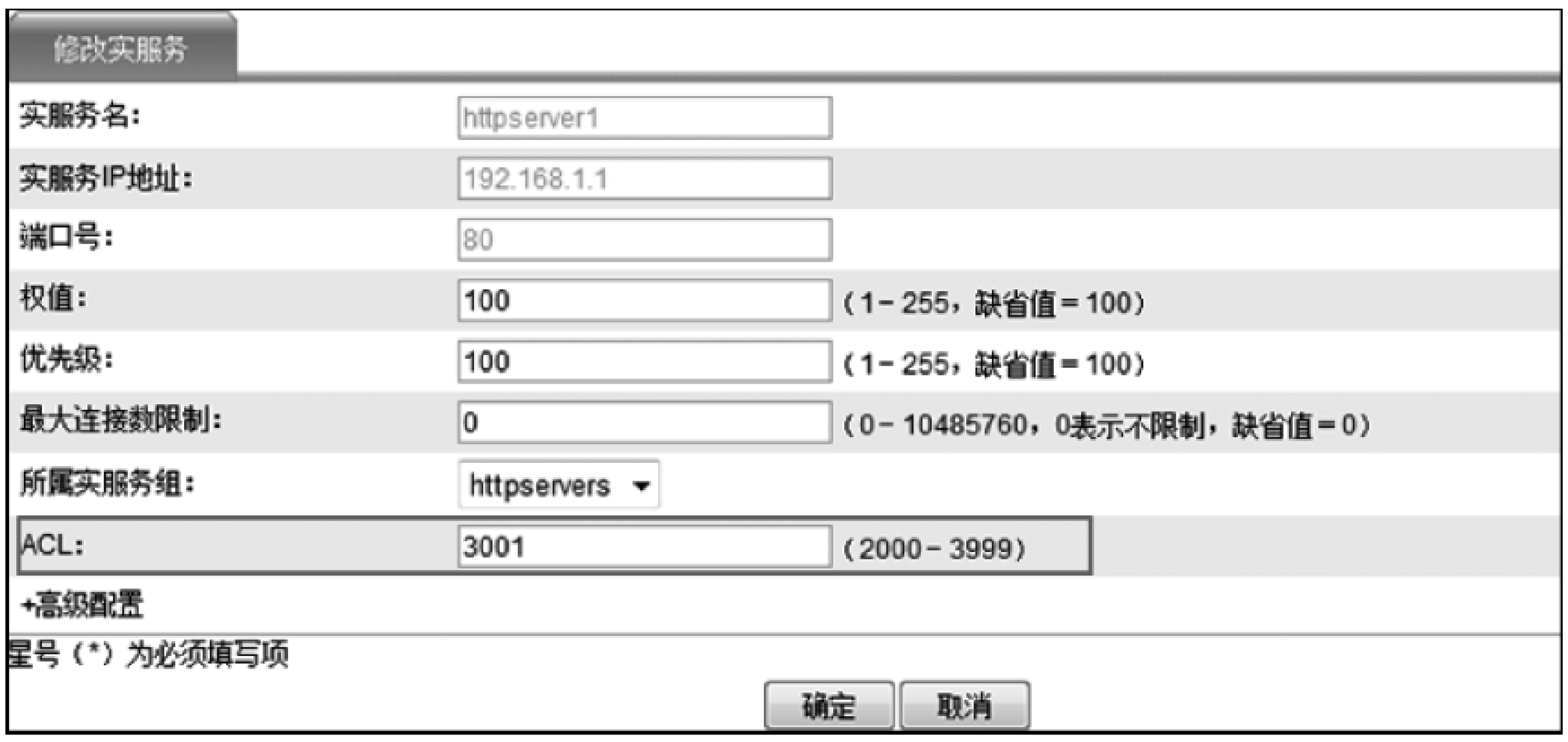
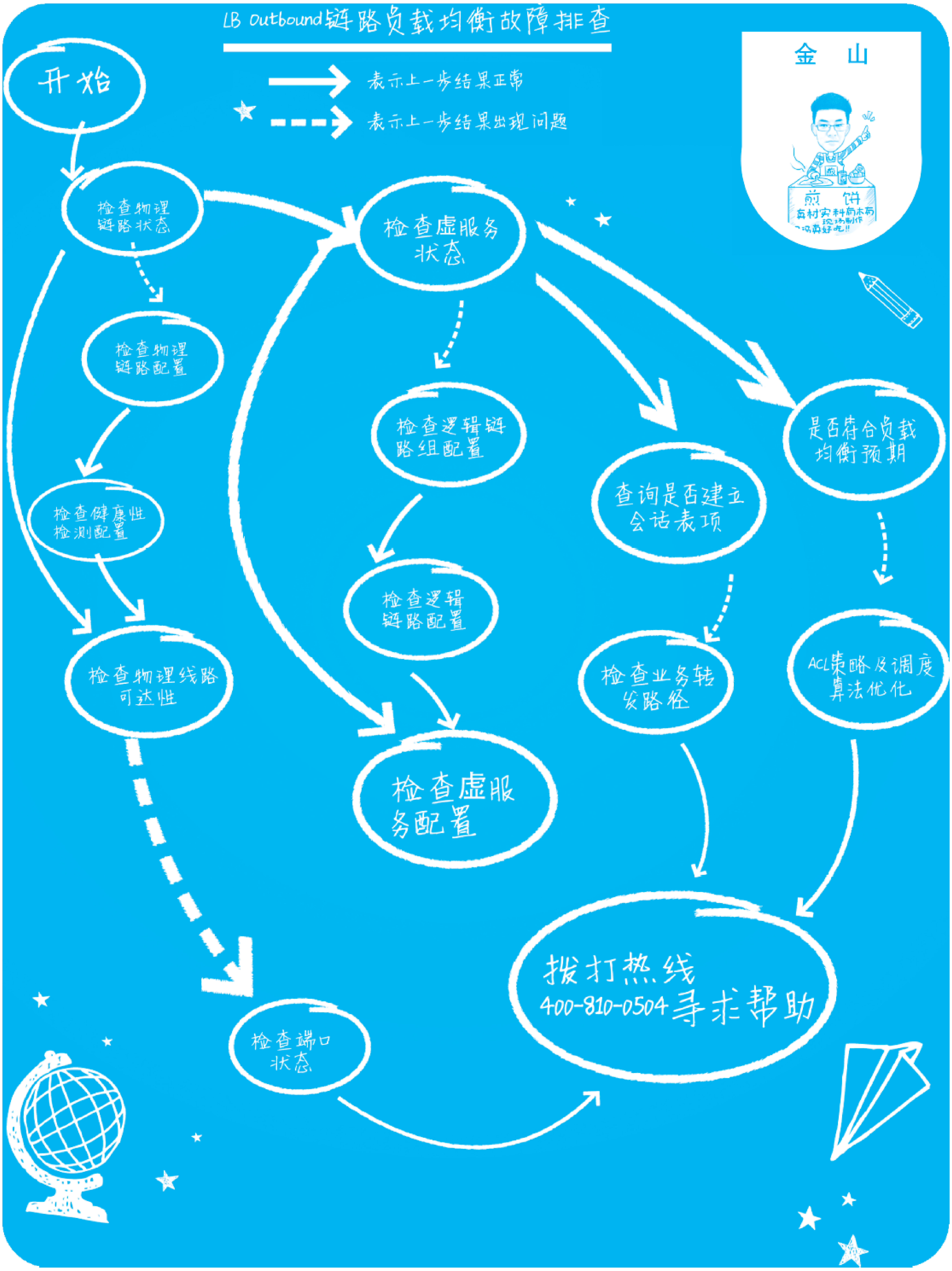


图 6-139　修改实服务

然后在命令行下面通过会话查看 LB 根据 ACL 策略分发的效果，可以看到 LB 已经将 10.0.0.10 的流量分发给 192.168.1.1 这台实服务。

```
[H3C]display session table source-ip 10.0.0.10 destination-ip 60.191.99.142 verbose
Initiator:
Source IP/Port   : 10.0.0.10/51007
  Dest IP/Port   : 60.191.99.142/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
Source IP/Port   : 192.168.1.1/80
  Dest IP/Port   : 10.0.0.10/51007
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)      App: HTTP             State: FIN-CLOSE
Start time: 2013-04-27 06:40:37   TTL: 2s
Root                         Zone(in):
                             Zone(out):
Received packet(s)(Init): 4 packet(s) 172 byte(s)
Received packet(s)(Reply): 4 packet(s) 749 byte(s)
```


LB Outbound链路负载均衡故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查物理链路状态
检查物理链路配置
检查健康性检测配置
检查物理线路可达性
检查端口状态
检查虚服务状态
检查逻辑链路组配置
检查逻辑链路配置
检查虚服务配置
查询是否建立会话表项
检查业务转发路径
是否符合负载均衡预期
ACL策略及调度算法优化
拨打热线 400-810-0504 寻求帮助
金 山
煎 饼

1. 开始

Outbound 链路负载均衡问题定位故障的思路是：先检查物理链路状态以确保负载均衡(以下简称 LB)设备与网络的连通性，检查健康性检测配置与状态；然后检查虚服务状态，并确认配置是否正确；最后通过会话表项确认分担效果。如果希望对链路分担效果做进一步优化，可根据实际组网需求，利用 ACL 策略等手段对调度结果进行修正。如果 LB 设备未收到业务报文，需网络管理员从整网流量转发路径角度入手，对其他网络设备进行分析排查。

2. 流程图相关操作说明

(1) 检查物理链路状态

链路负载均衡实施业务流量调度的基础是“物理链路”，因此必须确保其状态正常。在 LB Web 管理页面中，可以查看到物理链路的“下一跳”“接口”“状态”等信息，进行问题排查时应根据实际组网情况进行核对。如信息存在错误或“状态”显示为红色，Outbound 链路负载均衡将无法使用该链路承载业务流量，此时应对该物理链路的配置情况进行检查。

例如：在 LB Web 管理界面“负载均衡→链路负载均衡→物理链路”中，如图 6-140 所示，检查各物理链路对应的接口、下一跳、状态等信息是否正确。

名称	VPN 实例	下一跳	健康性检测方法数	上行带宽（Mbps）	上行带宽繁忙比例(%)	下行带宽（Mbps）	下行带宽繁忙比例(%)	链路成本	ISP	状态	接口	操作
CNC		172.16.20.1	2	100	85	100	85	0	中国联通	●	Ten-GigabitEthernet0/0.20	
CTC		172.16.10.1	2	100	85	100	85	0	中国电信	●	Ten-GigabitEthernet0/0.10	
LAN		172.31.255.1	0	4000	70	4000	70	0		●	Ten-GigabitEthernet0/0.4000	

图 6-140 物理链路

(2) 检查物理链路配置

“物理链路”的配置包括名称等诸多重要参数。物理链路的名称应尽量明确、便于理解。下一跳通常为 LB 三层直联的对端设备接口地址，与 Internet 互联链路的下一跳通常为 ISP 线路网关地址，与内网互联链路的下一跳通常为指向内网方向的路由表项下一跳地址。在检查下一跳时，应同时检查接口是否正确。物理链路的名称、下一跳信息不能编辑，如需修改可先将配置错误的物理链路删除后，重新创建一条新的物理链路。上下行带宽配置应与 ISP 线路提供的实际带宽值相符；LB 与内网互联所对应的物理链路带宽值保持默认值即可。带宽繁忙比例参数的设置与带宽繁忙保护功能相关，网络管理员可适当进行调整，但不建议将比例设置过高，甚至超过 90%。在 ISP 选项中，可设置物理链路对应的运营商类型，该功能必须在导入专用 ISP 地址表项文件后方可启用，具体操作方法不在本云图的讨论范围内。一般情况下，除带外管理端口外，LB 启用了多少个三层业务口，就应该配置多少条物理链路与之一一对应。对于连接 ISP 的物理链路，可启用健康性检测功能以实时探测线路状态，若健康性检查功能探测失败，说明该 ISP 线路可能存在故障，LB 将主动禁用该物理链路，将业务流量调度至其他可用线路，同时还将向信息中心输出线路“Block”告警日志。健康性检测功能支持在单条物理链路上同时启用多种探测方法，通常设置为当其中任一种方法探测成功时即认为该线路

正常，从而避免出现频繁的线路阻塞与恢复。对于 LB 与内网互联对应的物理链路，因其稳定性较好，推荐不启用健康性检测以减少探测流量。

例如：在 LB Web 管理界面“负载均衡→链路负载均衡→物理链路”中，单击“操作”列中的“编辑”按钮，进入“修改物理链路”页面，对配置参数进行检查与修改，如图 6-141 所示。



图 6-141　修改物理链路

（3）检查健康性检测配置

LB 默认配置预定义了“icmp”“tcp_half_open”两种方法用于物理链路的健康性检测，启用后 LB 默认向该物理链路配置的“下一跳”地址进行探测。若网络管理员希望对远端跨网段的其他 IP 地址进行探测，可自定义检测方法并在物理链路配置中进行引用。若当前物理链路为失效状态，并且引用了自定义检测方法，那么就需要检查其配置是否正确，另外还要注意确认被检测 IP 是否能够响应 icmp、tcp_half_open 类型的探测报文。

例如：在 LB Web 管理界面“负载均衡→健康性检查”中，单击“操作”列中的“编辑”按钮，进入“修改健康性检查”页面，对配置参数进行检查与修改。在图 6-142 中，客户希望对 CTC 物理链路除下一跳地址外，对该线路相应的 DNS 服务器可达性做同步探测，服务器 IP 地址以 x. x. x. x 示意。

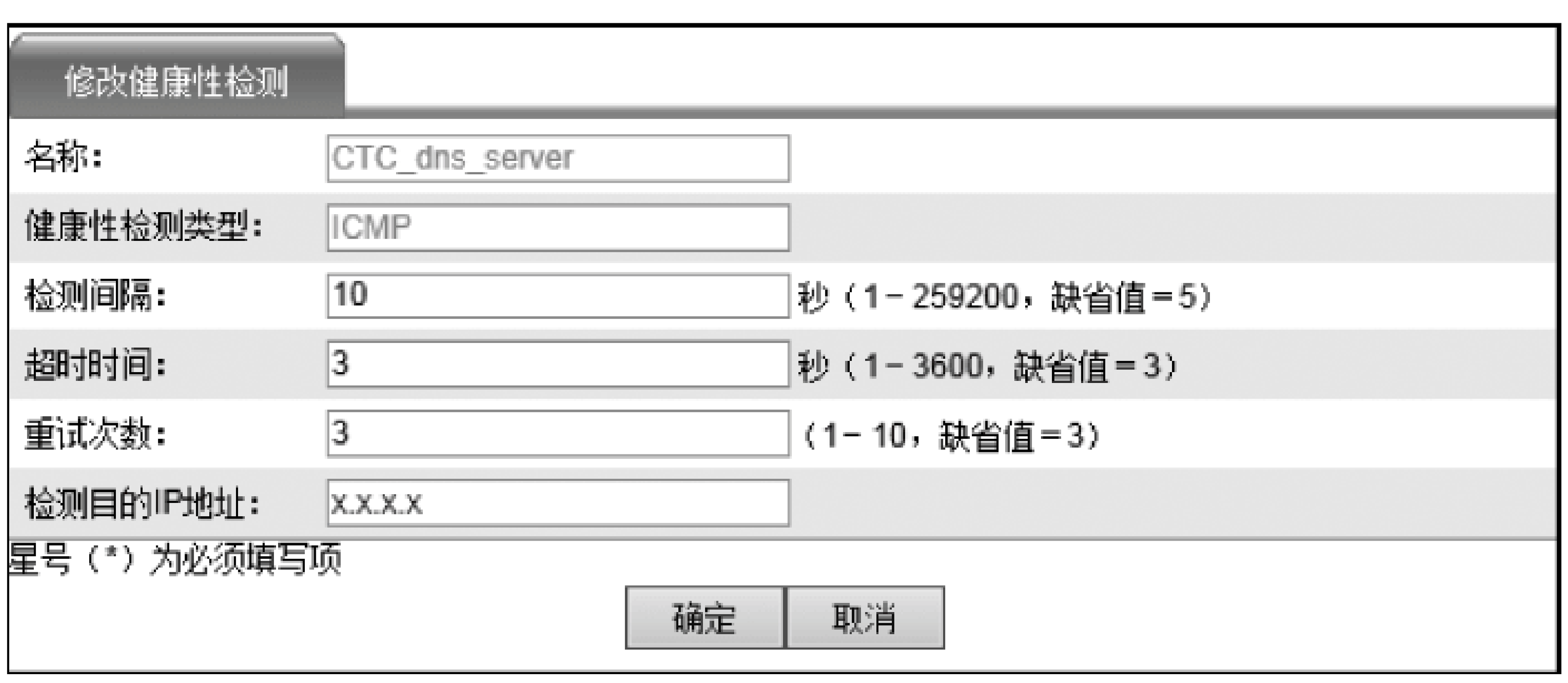


图 6-142　修改健康性检测

（4）检查物理线路可达性

查看 LB 设备的 ARP、路由表等网络可达性信息，通过 ping 测试等方法确认 LB 与其他网

络设备互联互通正常。需注意：即使正常状态下LB接收业务流量后是通过查找虚服务并调度转发的，但依然要确保LB上正确学习了全部的网络可达性信息，比如为LB配置了完整的静态路由表。

命令：*display arp*

例如：在CLI界面查看ARP表项学习是否正确，IP对应MAC地址是否正确。

```
[H3C] display arp
                Type: S-Static    D-Dynamic
IP Address      MAC Address       VLAN ID   Interface          Aging Type
172.16.10.1     000f-e280-de93    N/A       XGE0/0.10          20    D
172.16.20.1     000f-e280-de93    N/A       XGE0/0.20          20    D
172.31.255.1    3ce5-a682-c521    N/A       XGE0/0.4000        20    D
```

(5) 检查端口状态

检查LB各三层接口的速率、双工协商状态及对端状态是否正常，接口收发报文统计是否合理，是否存在错包，是否存在大量TTL超时报文(通常是路由环路造成)等。插卡形态的LB主要利用与宿主路由交换主机的内联万兆口承载业务流量，推荐采用三层子接口的部署方式并使能子接口速率统计功能，从而使LB插卡也可以实时统计承载在各个子接口上的业务流量带宽使用情况。

命令：*display interface interface-type interface-number*

例如：在CLI界面查看LB插卡内联口状态，子接口速率统计功能已使能。

```
<H3C> display interface Ten-GigabitEthernet 0/0
Ten-GigabitEthernet0/0 current state: Up
Line protocol current state: Up
Description: Ten-GigabitEthernet0/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 3ce5-a613-ff0c
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 3ce5-a613-ff0c
Media type is twisted pair, loopback not set, promiscuous mode not set
10Gb/s, Full-duplex, link type is force link
Output flow-control is disabled, input flow-control is disabled
Last clearing of counters: Never
    Peak value of input: 15677 bytes/sec, at 2000-4-26 15:23:11
    Peak value of output: 15606 bytes/sec, at 2000-4-26 15:23:11
    Last 5 seconds input rate 12994 bytes/sec, 103952 bits/sec, 127 packets/sec
    Last 5 seconds output rate 13015 bytes/sec, 104120 bits/sec, 127 packets/sec
    Input: 36427 packets, 0 jumboes, 2742408 bytes, 36427 buffers
           16014 broadcasts, 14412 multicasts, 0 pauses
           0 errors, 0 runts, 0 giants
           0 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
    Output:9822 packets, 787464 bytes, 9822 buffers
           3826 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 underruns, 0 collisions
           0 deferred, 0 drops, 0 lost carriers

<H3C>display interface Ten-GigabitEthernet 0/0.10
Ten-GigabitEthernet0/0.10 current state: Up
Line protocol current state: Up
Description: Ten-GigabitEthernet0/0.10 Interface
```

```
The Maximum Transmit Unit is 1500
Internet Address is 172.16.10.254/24 Primary
IP Packet Frame Type: PKTFMT_ETHNT_2,   Hardware Address: 3ce5-a613-ff0c
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,   Hardware Address: 3ce5-a613-ff0c
 Last clearing of counters:   Never
 Last 5 seconds input   rate : 73 packets/sec , 7486 bytes/sec
 Last 5 seconds output rate : 76 packets/sec , 7772 bytes/sec
     Input : 2603 packets , 264346 bytes
     Output: 3566 packets , 363452 bytes
```

(6) 检查虚服务状态

在 Outbound 链路负载均衡中，当 LB 接收到业务报文后，会首先将其与当前会话表项进行查找匹配，若不能与任何一条会话表项匹配，LB 会将该报文与所有状态可用的虚服务进行匹配，以决定最终通过哪条虚服务执行调度并创建会话表项。若排查时发现某条虚服务呈不可用状态(红色)，则该虚服务将不能用于上述指导业务流量调度的工作。

在问题分析时，网络管理员可以预先判断业务流量将通过哪条虚服务进行调度，具体方法如下：假设当前有多条虚服务均处于可用状态，可将新发起连接的业务首报文与“IP 地址方式”“ACL 方式”中配置的全部虚服务进行比对，推断报文将命中哪个虚服务进行调度。前者执行最长匹配方式，后者执行优先级顺序匹配方式，且 IP 地址方式虚服务总体优先于 ACL 方式虚服务，特别地，进行虚服务匹配时，如果 LB 上当前还有生效的服务器负载均衡虚服务，则必须将这类虚服务与 IP 地址方式的虚服务合并后按最长匹配方式进行匹配。如果 LB 上配置有 NAT Outbound，LB 处理顺序为先执行调度后做 NAT；如果 LB 上配置有 NAT Server，LB 的处理顺序为先做 NAT 后执行调度；NAT Static 在 Outbound 方向与前者处理顺序相同，在反方向与后者处理顺序相同。

例如：在 LB 设备 Web 管理界面“负载均衡→链路负载均衡→Outbound→虚服务”中，检查虚服务状态。在图 6-143 中，假设未配置“ACL 方式”虚服务和服务器负载均衡虚服务，则业务流量都将以会话首报文目的 IP 地址与虚服务执行最长匹配，“VS_LAN”对应目标地址为内网 IP(10.0.0.0/8)的会话流量，“VS_Internet”对应其余所有会话流量。



图 6-143　虚服务配置

(7) 检查逻辑链路组配置

在出方向链路负载均衡中，每个逻辑链路组与虚服务一一对应。若逻辑链路组中仅包含一条逻辑链路，调度算法选择默认的“轮转”算法即可；若逻辑链路组中包含两条或两条以上逻辑链路，调度算法建议选择“源地址散列”，以确保来自内网同一个源 IP 发起的业务流量不会被分散调度至多条 ISP 线路，避免网银类应用出现问题(此类应用通常在整个交互过程中不

允许客户端地址出现变化)。其他调度算法常用于服务器负载均衡场景,在 Outbound 链路负载均衡中很少采用。“逻辑链路故障处理”采用默认配置“保持已有连接”即可。高级配置中的“温暖上线”功能也主要用于服务器负载均衡场景,在 Outbound 链路负载均衡中建议不使能。

例如:在 LB 设备 Web 管理界面“负载均衡→链路负载均衡→Outbound→逻辑链路组”中,检查逻辑链路组配置情况,如图 6-144 所示。

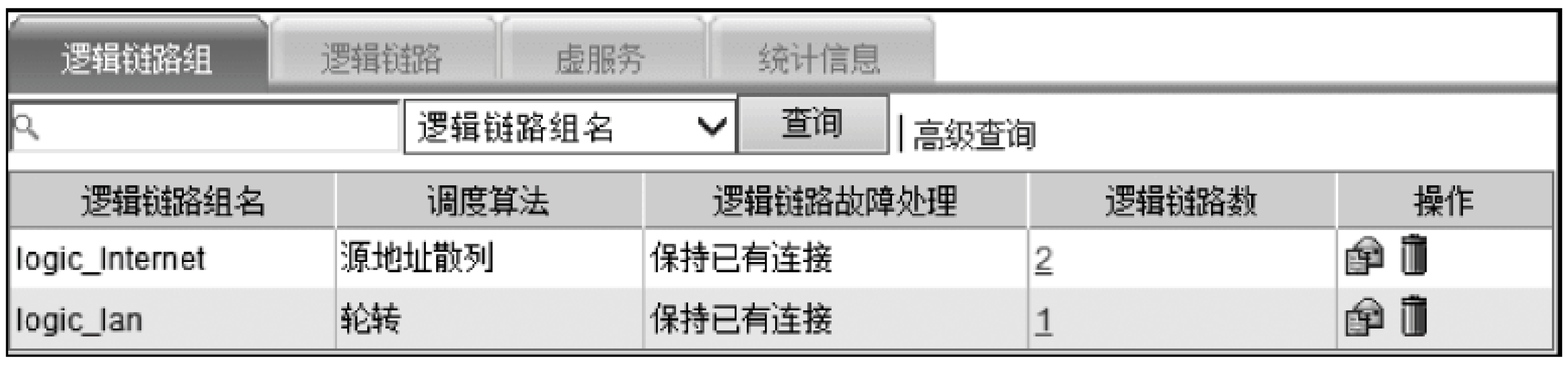


图 6-144　逻辑链路组

例如:若配置存在错误,可单击“操作”列中的“编辑”按钮,进入“修改逻辑链路组”页面,重新进行配置,如图 6-145 所示。

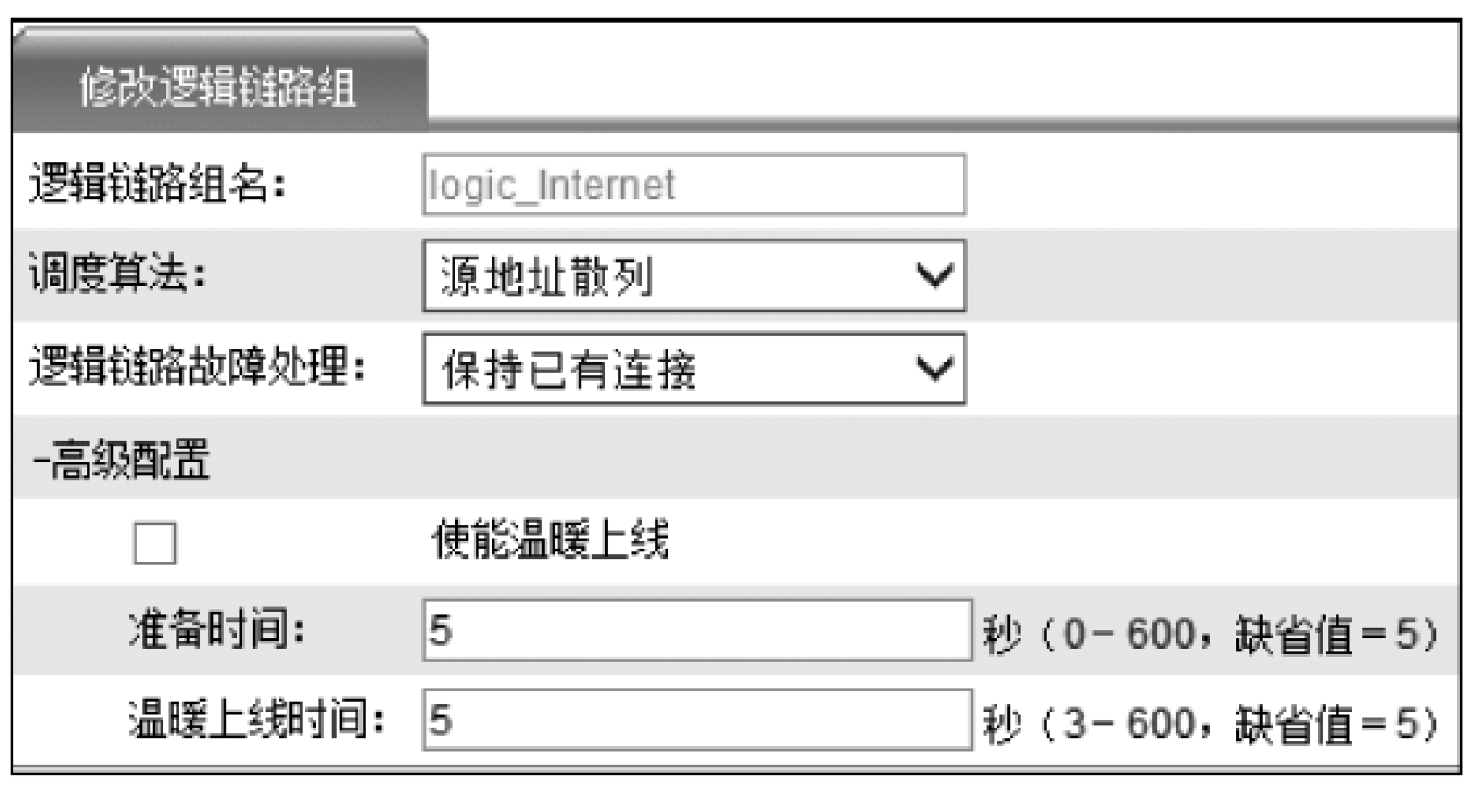


图 6-145　修改逻辑链路组

(8)检查逻辑链路配置

在 Outbound 链路负载均衡中,逻辑链路主要用于在物理链路与逻辑链路组之间建立联系,实现单条物理链路可被多个不同“逻辑链路组——虚服务”所引用。在进行配置检查时,需重点查看逻辑链路所加入的逻辑链路组及其对应的物理链路是否准确,是否符合组网预期。若逻辑链路上配置了 ACL 策略,则 LB 在进行选路调度时,会根据 ACL 规则强制将新建会话流量从这条逻辑链路所对应的物理链路上发送。在其他配置参数中,“权值”常用于表达同一运营商多条线路之间的带宽比。通过“权值”与“ISP 选路”功能、“源地址散列”算法相互配合,LB 可以实现将业务流量调度至同一运营商提供的多条物理链路时,按带宽比进行分担。“优先级”参数用于和“本地优先级”调度算法配合使用,若未使用该调度算法,则“优先级”参数保持默认值即可。“最大连接数限制”参数可以控制单个逻辑链路上分担的最大会话数,默认设置为“0”表示不作限制。“状态”表达了该逻辑链路当前是否能够分担业务流量,正常情况为“绿色”可用状态,需注意,如果未配置或未使能其所属逻辑链路组对应的虚服务,或启用了高级配置中的“使能慢宕”“立即停止服务”“停止调度”等选项时,逻辑链路的当前状态将转变为其他非正常状态。

高级配置中的“使能慢宕”选项启用后,逻辑链路将仅处理已经分配至本线路转发的会话流量,LB 不会再向本逻辑链路调度新的会话流量;当逻辑链路上已有会话全部老化后,本逻辑链路即平滑退出逻辑链路组,从而避免业务流受影响。相对地,如果启用“立即停止服务”选

项，本逻辑链路将立刻停止所有转发。“停止调度”选项启用后，本逻辑链路将不再参与就近性、ISP 选路和算法调度，此时只能通过 ACL 策略牵引业务流量经本线路转发，相当于将该逻辑链路对应的物理链路视为“专线”使用，不再参与动态调度。关于上述高级选项的详细配置指导可查询 LB 产品用户手册。

例如：在 LB 设备 Web 管理界面“负载均衡→链路负载均衡→Outbound→逻辑链路”中，检查逻辑链路配置情况，检查其状态是否正常，如图 6-146 所示。



图 6-146　逻辑链路

例如：若发现配置有误，可单击“操作”列中的“编辑”按钮，进入“修改逻辑链路”页面，重新设置逻辑链路的各项参数，如图 6-147 所示。

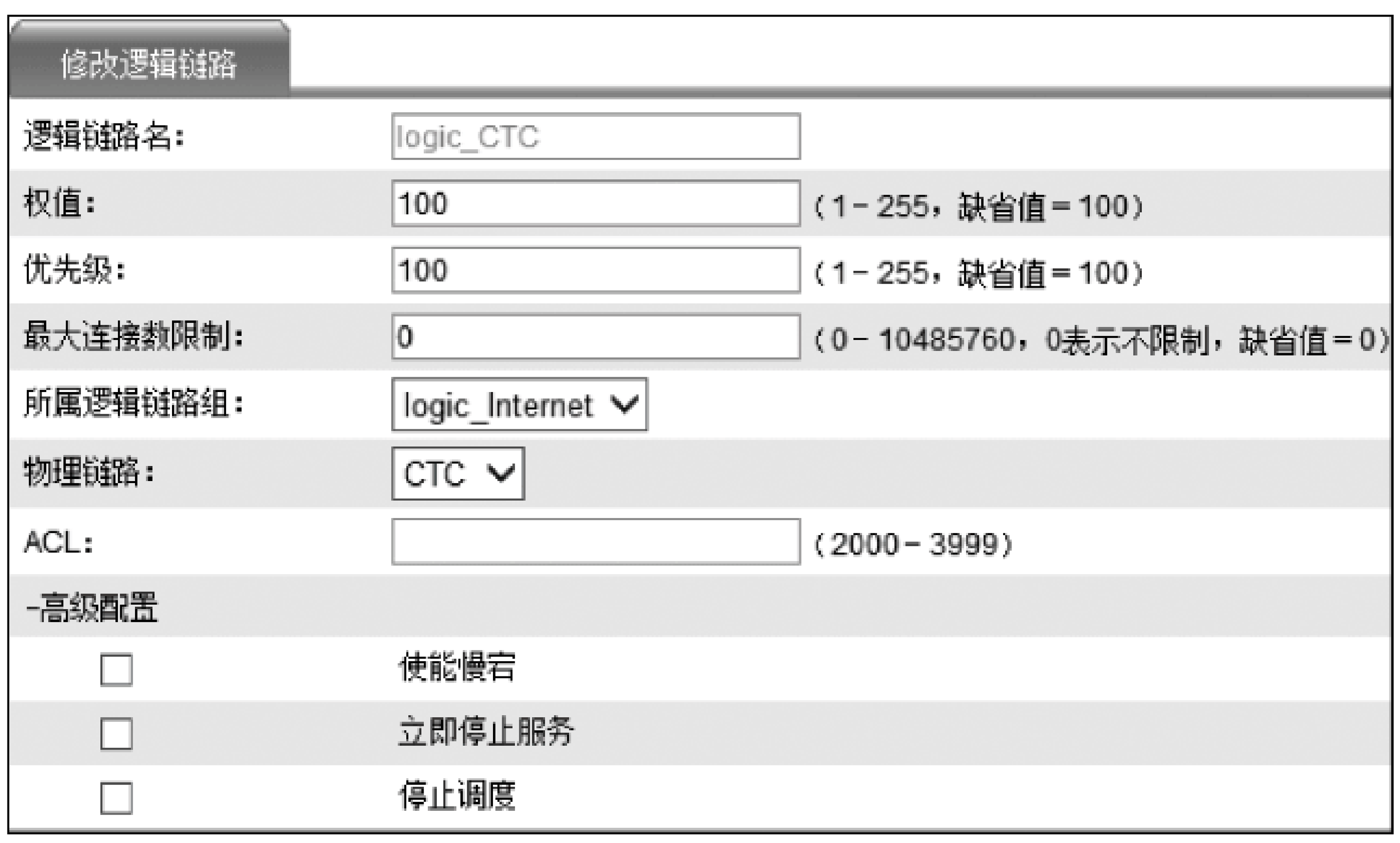


图 6-147　修改逻辑链路

(9) 检查虚服务配置

Outbound 链路负载均衡根据虚服务匹配方式，分为“IP 地址方式”“ACL 方式”两种。前者将会话首报文中目的 IP 地址与“虚服务 IP 地址/掩码”(包含服务器负载均衡中配置的全部虚服务)执行最长匹配，以决定该新建会话将按哪条虚服务进行调度，这个过程与路由器执行三层转发时查找路由表类似；而后者则将 ACL 规则按优先级顺序与会话首报文进行匹配，以决定该新建会话将按哪条 ACL 所对应的虚服务进行调度。因此，在进行配置检查时，除了检查虚服务状态是否正常、对应的逻辑链路组等配置是否正确、是否与服务器负载均衡虚服务存在冲突以外，对于“IP 地址方式”类型的虚服务，还应重点检查虚服务 IP 地址/掩码、协议类型、端口号是否正确，对于“ACL 方式”类型的虚服务，还应重点检查虚服务对应的 ACL 规则是否正确，优先级设置是否合理等。

因“IP 地址方式”虚服务更优先，为避免配置冲突，不建议同时使用“IP 地址方式”和

“ACL 方式”进行虚服务配置。若当前设备软件版本支持，推荐使用“ACL 方式”进行配置，在引用的 ACL 规则中应该尽可能精确(如指定业务发起方源 IP 地址/掩码)，避免无关业务或攻击流量匹配虚服务后，被 LB 执行调度，浪费资源与带宽。

Outbound 链路负载均衡中，LB 通过多种方式决策业务流量最终将调度至哪条物理链路时，优先顺序由高至低依次为：持续性>ACL 策略>就近性>ISP 表项>调度算法。

关于“就近性”“ISP 选路”“链路带宽繁忙保护”等高级特性的配置指导及应用场景，可查询 LB 产品用户手册。

例如：在 LB 设备 Web 管理界面“负载均衡→链路负载均衡→Outbound→虚服务”中，检查虚服务配置。在图 6-148 中，采用“IP 地址方式”进行配置，“VS_LAN”对应目标地址为内网 IP(10.0.0.0/8)的会话流量，“VS_Internet”对应其余所有会话流量。



图 6-148　虚服务配置

例如：若发现配置有误，可单击“操作”列中的“编辑”按钮，进入“修改虚服务”页面，重新设置虚服务的各项参数。部分配置不支持直接修改，可删除后重新创建虚服务，如图 6-149 所示。



图 6-149　虚服务配置

(10) 查询是否建立会话表项

通过查看 LB 会话表项信息，可以观察业务流量在 LB 上的具体调度情况。为了更直观地判断报文的入/出端口，可以利用安全区域特性：将 LB 内网接口加入“LAN”区域，将各个 ISP

接口分别加入诸如“CTC”“CNC”“CMCC”等区域，查看会话表项详细信息时，便可以通过源/目的安全区域得知这条业务流是从哪个端口主动发起，以及 LB 将其调度至哪个 ISP 线路发出。默认配置下，LB 的业务端口未添加安全区域属性，但不影响报文的正常转发，这一点与防火墙设备有很大不同。

若 LB 设备上无法查找到业务流对应的会话表项，需确认业务报文是否已经发出。一种常见原因是整网业务流量规划错误，造成业务报文未经过 LB 转发。

例如：在 LB 设备 Web 管理界面“安全特性→会话管理→会话列表”中，设置查询条件为会话发起方源 IP 地址 10.255.254.101，然后单击“查询”按钮，即可查询对应的会话表项。本例中，如图 6-150 所示，可以观察到源 IP 地址 10.255.254.101 向目的 IP 地址 10.255.254.13 主动发起了一个 ICMP 协议的数据流。

查询项：发起方源IP地址　IP地址：10.255.254.101　查询

□	发起方源IP地址	发起方目的IP地址	发起方VPN/VLAN/INLINE	响应方源IP地址	响应方目的IP地址	响应方VPN/VLAN/INLINE	协议	会话状态	存活时间(秒)	操作
□	10.255.254.101:2048	10.255.254.13:16	---	10.255.254.13:0	10.255.254.101:16	---	ICMP	ICMP-CLOSED	29	

图 6-150　发起方源 IP 地址

例如：通过单击“操作”列中的“查看”按钮，进入“会话详细信息”页面，在该页面中可以观察到这条数据流的接收处理情况。如图 6-151 所示，通过安全区域信息，可以得知 LB 从“LAN”区域对应端口接收了会话正向报文，并将流量调度至“CTC”区域对应端口发出；LB 也正常接收处理了会话反向报文，正反方向报文个数均为 3868 个。

会话详细信息

Protocol：ICMP　State：ICMP-CLOSED　TTL (S)：30

Initiator: VD / ZONE / VPN / IP / PORT		Responder: VD / ZONE / VPN / IP / PORT	Packets	Bytes
Root / LAN / --- / 10.255.254.101 / 2048	--------->	Root / CTC / --- / 10.255.254.13 / 16	3868	324912
Root / LAN / --- / 10.255.254.101 / 16	<---------	Root / CTC / --- / 10.255.254.13 / 0	3868	324912

图 6-151　会话详细信息

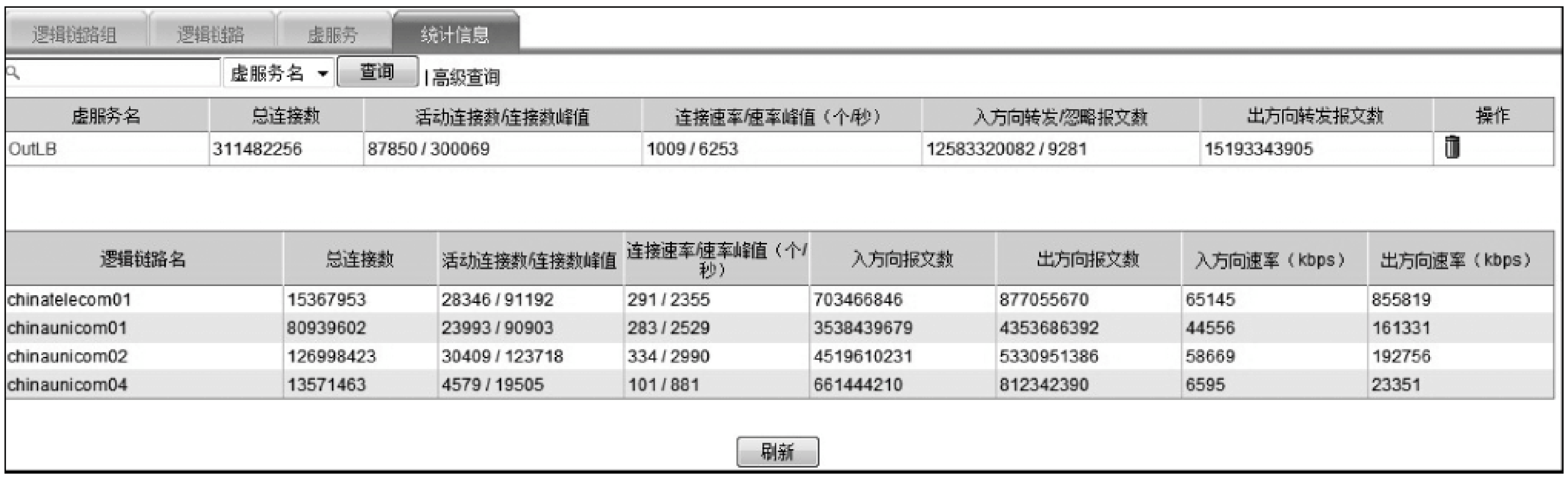
（11）检查业务转发路径

若业务报文确已发出，但 LB 设备上始终无法查询到对应的会话表项，则通常是由于业务流量实际未经 LB 转发导致。针对这种情况，建议从业务发起方开始，对整网流量路径规划进行逐跳检查。

（12）是否符合负载均衡预期

网络管理员利用会话表项信息可以确认实际业务经过 LB 调度后的转发情况。利用虚服务统计信息可以观察各物理链路的带宽使用情况，其中“入方向”指会话表项正方向，“出方向”指会话表项反方向。以内网访问 Internet 的“全零”虚服务为例，“入方向”即内网访问 Internet 的上行流量方向，“出方向”即从 Internet 返回的下行流量方向。

例如：如图 6-152 所示，在 LB 设备 Web 管理界面“负载均衡→链路负载均衡→Outbound→统计信息”页签中，可以直观地看到“OutLB”虚服务所包含的四条逻辑链路的流量分担情况。



虚服务名	总连接数	活动连接数/连接数峰值	连接速率/速率峰值（个/秒）	入方向转发/忽略报文数	出方向转发报文数	操作
OutLB	311482256	87850 / 300069	1009 / 6253	12583320082 / 9281	15193343905	

逻辑链路名	总连接数	活动连接数/连接数峰值	连接速率/速率峰值（个/秒）	入方向报文数	出方向报文数	入方向速率（kbps）	出方向速率（kbps）
chinatelecom01	15367953	28346 / 91192	291 / 2355	703466846	877055670	65145	855819
chinaunicom01	80939602	23993 / 90903	283 / 2529	3538439679	4353686392	44556	161331
chinaunicom02	126998423	30409 / 123718	334 / 2990	4519610231	5330951386	58669	192756
chinaunicom04	13571463	4579 / 19505	101 / 881	661444210	812342390	6595	23351

图 6-152　统计信息

（13）ACL 策略及调度算法优化

若业务调度不符合组网规划预期，网络管理员可以通过调整 ACL 策略、调度算法等手段对调度效果进行调整。例如，客户希望内部服务器区网段所有访问 Internet 的流量都固定从某条物理链路发出，可通过配置 ACL 策略实现。

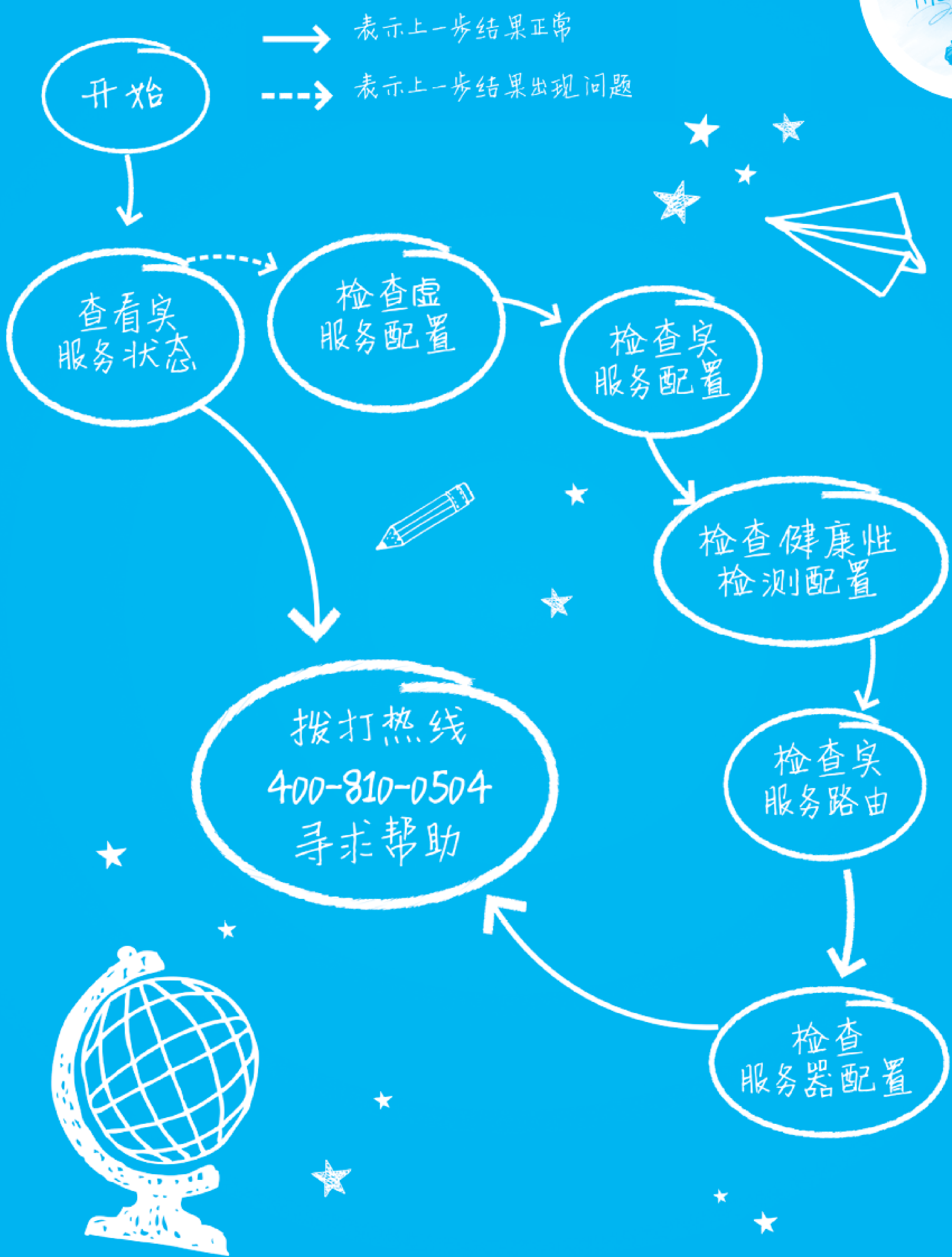
一般场景下，Outbound 链路负载均衡的推荐部署方案为：以 ACL 方式进行虚服务配置，指向 Internet 的虚服务引用匹配源 IP 为内网地址的 ACL 规则，指向内网的虚服务引用匹配目的 IP 为内网地址的 ACL 规则，为连接 Internet 的物理链路选择对应的 ISP 属性并启用“ISP 选路”特性，启用链路带宽繁忙保护功能，调度算法选择“源地址散列”，针对需要固定转发路径的流量通过 ACL 策略手工指定其分担线路。“持续性”“就近性”功能无须启用。具体配置指导可查询 LB 产品用户手册。

对于复杂组网需求，需灵活运用 LB 产品各功能特性，可及时向 H3C 技术支持工程师咨询。

LB健康性检测故障排查

翟运波





1. 开始

LB 通过健康性检测实时监控服务器或者链路的状态，以保证整个业务的高可靠性。以服务负载分担为例，健康性检测定位故障的思路是：先查看实服务状态，然后检查虚服务状态是否使能，接着检查实服务及其健康性检测配置，再检查服务器路由，最后检查服务器的端口、应用程序等是否正常。

2. 流程图相关操作说明

（1）查看实服务状态

LB 通过健康性检测实时监控各实服务的状态，状态正常的实服务显示绿灯●，一旦检测到实服务故障或者人为停止服务，就显示为红灯⊘，如果使实服务进入慢宕状态，实服务显示红绿相间的灯●。LB 不会向故障的实服务分发流量，在日常维护过程中要及时关注实服务的状态。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“实服务”页签，如图 6-153 所示，可以看到 dnsserver1 和 dnsserver2 状态不正常，httpserver1 开启了慢宕，httpserver2 的状态正常。



图 6-153　实服务

（2）检查虚服务配置

对于服务器负载分担，只有使能虚服务以后才会触发实服务的健康性检测，否则实服务一直显示红灯。所以，如果实服务的状态不正常，请首先检查虚服务是否已经使能，如果已经使能，则状态显示绿灯●；如果虚服务没有使能则状态显示红灯⊘。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“虚服务”页签，然后单击对应虚服务后面的编辑按钮进入虚服务的配置界面，如图 6-154 所示，可以看到 dns_service 这个虚服务没有使能，状态显示红灯；http_service 这个虚服务已经使能，状态显示绿灯。

如果虚服务没有使能，可以单击虚服务后面的编辑按钮进入虚服务配置界面使能虚服务，如图 6-155 和图 6-156 所示。

（3）检查实服务配置

如果确认虚服务状态已经使能，需要仔细检查实服务的 IP 地址、端口等配置是否正确，有没有被人为停止服务。



图 6-154　虚服务



图 6-155　虚服务配置



图 6-156　修改虚服务

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“实服务”页签，然后单击对应实服务后面的编辑按钮进入实服务的配置界面，如图 6-157 和图 6-158 所示，看到实服务 httpserver1 的 IP 地址、端口配置正确，健康性检测方法和实服务组一致。

（4）检查健康性检测

LB 服务器负载中，每个实服务可以配置单独的健康性检测方法，也可以和所属实服务组的健康性检测方法一致，需要根据配置对相应的健康性检测方法进行排查。例如：对于



图 6-157 实服务配置



图 6-158 修改实服务

ICMP 检测方法，需要检查目的地址是否正确、LB 到实服务路由是否可达，服务器是否允许 ping 等操作；对于 HTTP 检测方法，需要检查服务地址、下载文件的路径和文件名称是否正确，对于 FTP 检测方法，需要检查 FTP 服务的地址、登录用户名/密码、文件路径和文件名称是否正确（默认情况下 LB 健康性探测的目的 IP 地址就是实服务的 IP 地址，还支持手工配置）。

例如：进入 LB 的 Web 管理界面，在导航栏中选择“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“实服务”页签，然后单击对应实服务后面的编辑按钮进入实服务的配置界面，看到 httpserver1 这个实服务的健康性检查选择的类型和实服务组一致，再单击“实服务组”页签，查看实服务组的健康性检测类型是 ICMP，然后进入 LB 的健康性检测配置页面检查 ICMP 的相关配置参数。同样的方法，可以调整 HTTP、FTP 等健康性检测方法的参数，过程如图 6-159～图 6-163 所示。

（5）检查实服务路由

LB 健康性探测报文以自己的接口地址有源地址，实服务的 IP 地址为目的地址，要保证健康性检测正常，LB 到实服务的路由必须正常。排查问题时要注意检查 LB 到实服务的路由，或者通过 ping 简单测试一下到实服务的可达性。

命令：*display ip routing-table x.x.x.x*



图 6-159　修改实服务

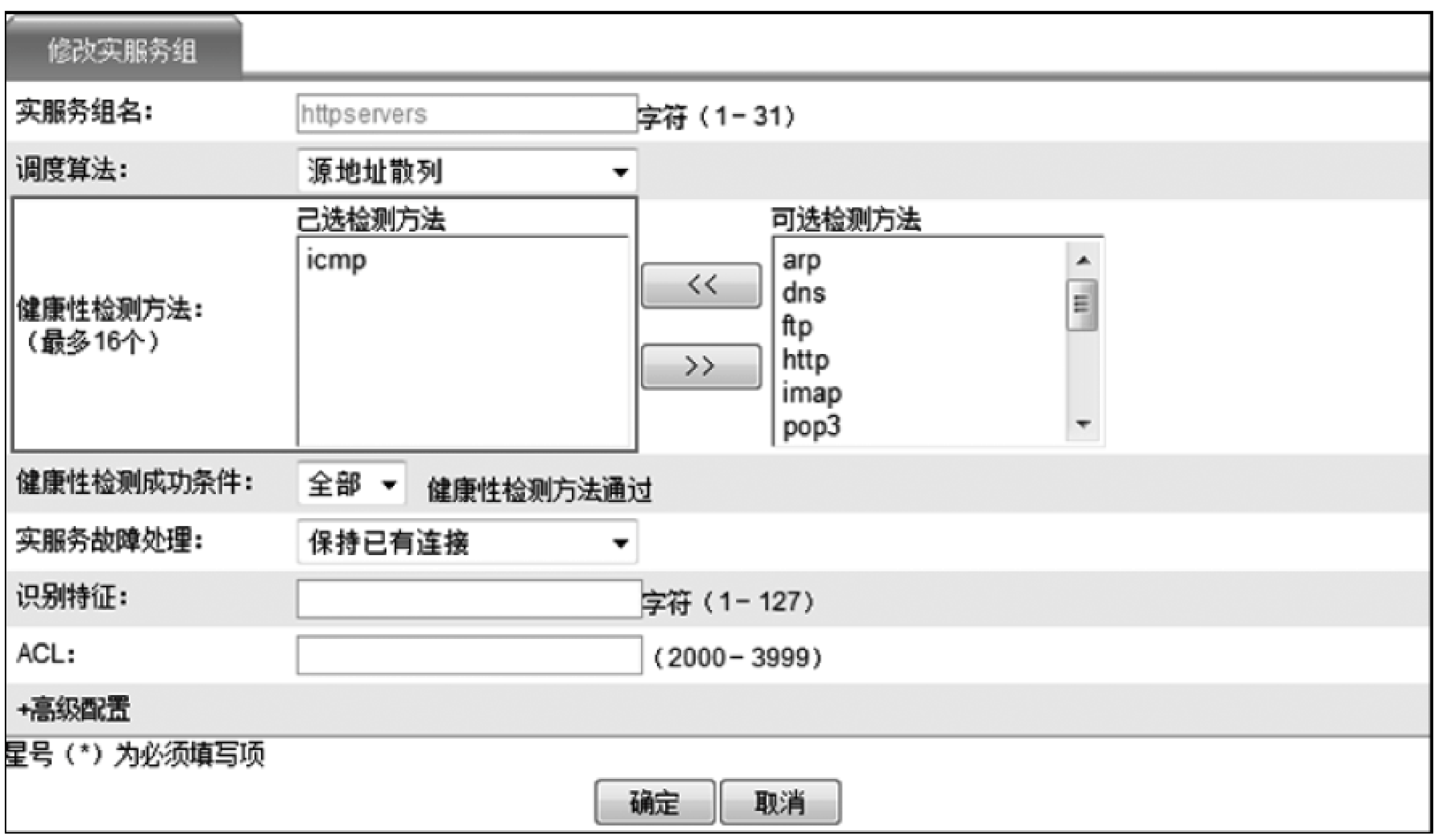


图 6-160　修改实服务组



图 6-161　修改健康性检测(1)

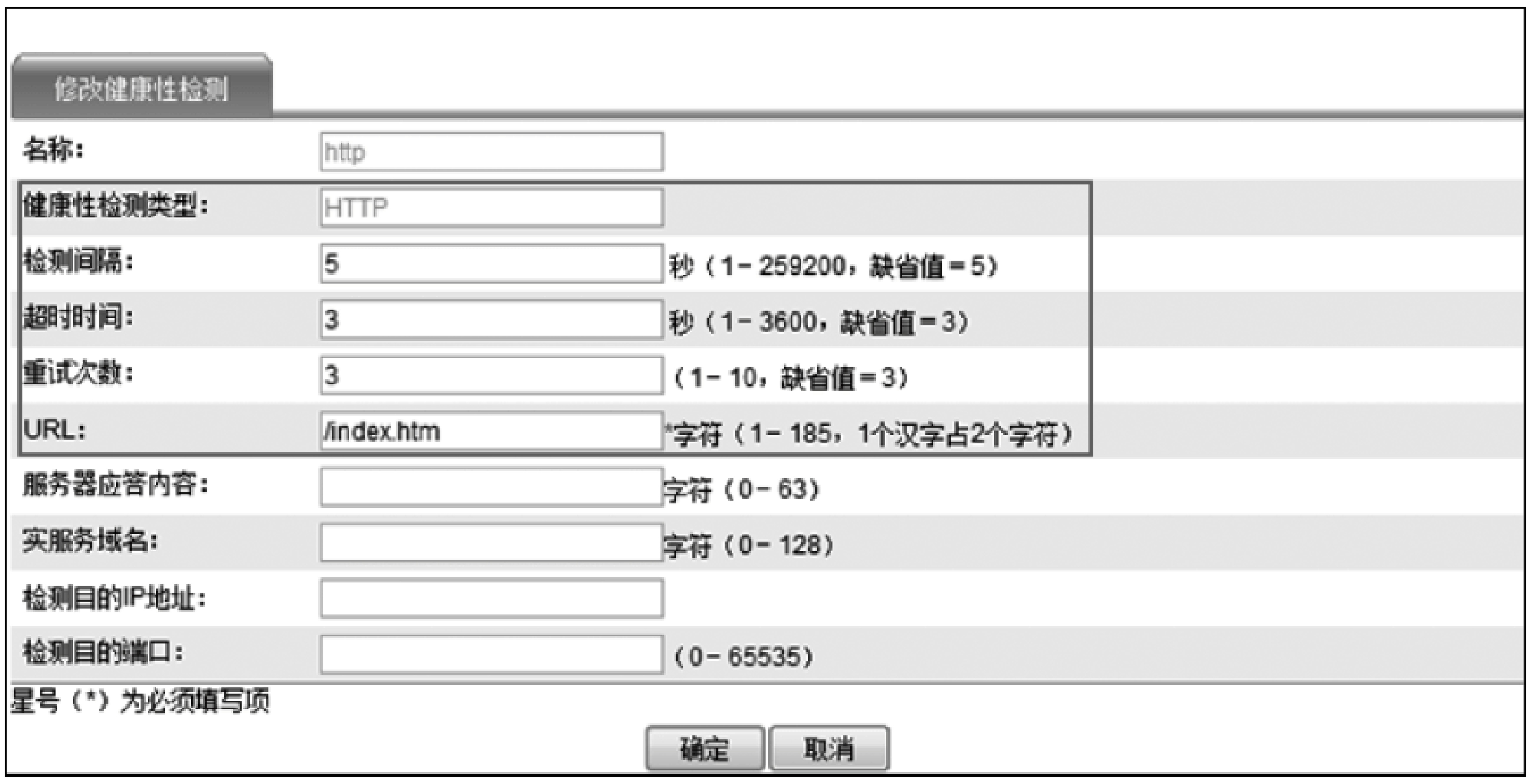


图 6-162　修改健康性检测(2)

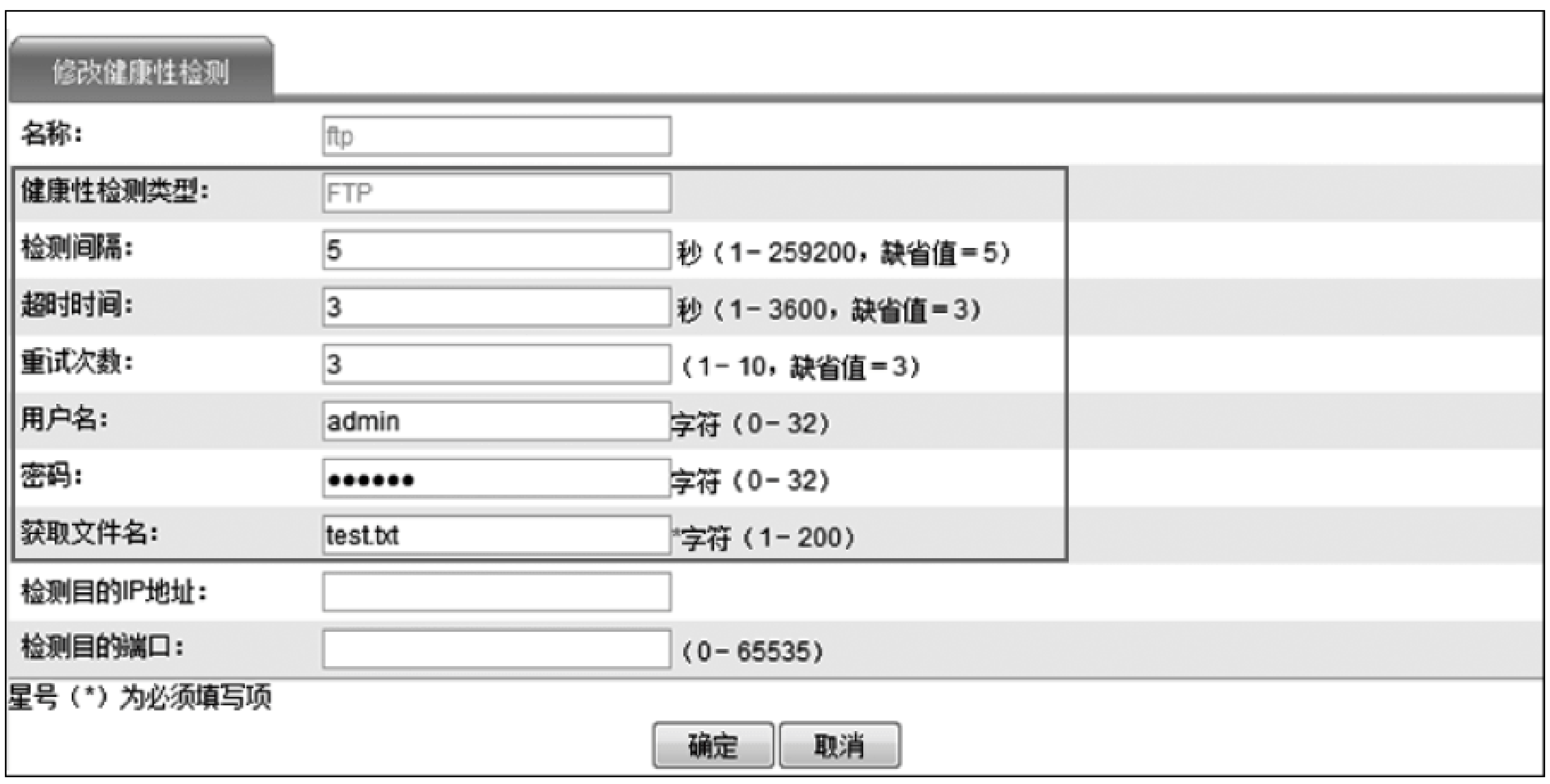


图 6-163　修改健康性检测(3)

例如：通过命令可以看到 LB 上到实服务 192.168.1.1 的路由正常，ping 测试可达。

```
<LB>display ip routing-table 192.168.1.1
Routing Table : Public
Summary Count : 1
Destination/Mask    Proto   Pre  Cost        NextHop         Interface
192.168.1.0/24      Direct  0    0           192.168.1.254   XGE0/0.50

<LB>ping 192.168.1.1
  PING 192.168.1.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=0 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
```

```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

（6）检查服务器配置

如果确认 LB 的配置和路由都正确，但是健康性检测还是失败的话，就需要排查下中间链路及服务器的配置了。先在服务器上抓包确认探测报文是否到达服务器，如果没有需要仔细检查中间设备路由情况，如果到达服务器，就需要检查服务提供业务的端口、应用程序等是否正常。

命令：*netstat -ano*

例如：以 Windows 服务器为例，进入服务器 CMD 运行界面，通过 netstat -ano 可以看到服务器 80 端口监听正常。

```
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation.保留所有权利.

C:\Users\z07119>netstat -ano

活动连接

  协议   本地地址            外部地址          状态          PID
  TCP    0.0.0.0:21          0.0.0.0:0         LISTENING     7996
  TCP    0.0.0.0:80          0.0.0.0:0         LISTENING     7368
  TCP    0.0.0.0:135         0.0.0.0:0         LISTENING     960
  TCP    0.0.0.0:445         0.0.0.0:0         LISTENING     4
  TCP    0.0.0.0:623         0.0.0.0:0         LISTENING     4544
  TCP    0.0.0.0:2425        0.0.0.0:0         LISTENING     4824
  TCP    0.0.0.0:16992       0.0.0.0:0         LISTENING     4544
  TCP    0.0.0.0:58927       0.0.0.0:0         LISTENING     768
```


LB Inbound链路负载均衡故障排查
表示上一步结果正常
表示上一步结果出现问题
金 山
煎 饼
开始
检查链路层及网络层可达性信息
检查物理链路配置
检查DNS重定向配置
DNS解析测试
拨打热线400-810-0504寻求帮助

1. 开始

Inbound 链路负载均衡问题定位故障的思路是：先检查物理链路状态以确保负载均衡(以下简称 LB)设备与网络的连通性，检查健康性检测配置与状态；然后检查 Inbound 负载均衡配置是否正确；对于需要 LB 设备固定应答 DNS 解析的需求，可通过配置 ACL 策略实现。配置检查完成后，可通过直接将 LB 指定为 DNS 服务器并进行解析测试，来判断 LB 能否正确应答 DNS 解析请求。

2. 流程图相关操作说明

(1) 检查物理链路状态

链路负载均衡实施业务流量调度的基础是“物理链路”，因此必须确保其状态正常。在 LB Web 管理页面中，可以查看到物理链路的“下一跳”“接口”“状态”等信息，应根据实际组网情况进行核对。如信息存在错误或“状态”显示为红色，Outbound 链路负载均衡将无法使用该链路承载流量，此时应对该物理链路的配置情况进一步进行检查确认。

例如：在 LB Web 管理界面“负载均衡→链路负载均衡→物理链路”中，检查各物理链路对应的接口、下一跳、状态等信息是否正确，如图 6-164 所示。

名称	VPN 实例	下一跳	健康性检测方法数	上行带宽（Mbps）	上行带宽繁忙比例(%)	下行带宽（Mbps）	下行带宽繁忙比例(%)	链路成本	ISP	状态	接口	操作
CNC		172.16.20.1	2	100	85	100	85	0	中国联通	●	Ten-GigabitEthernet0/0.20	
CTC		172.16.10.1	2	100	85	100	85	0	中国电信	●	Ten-GigabitEthernet0/0.10	
LAN		172.31.255.1	0	4000	70	4000	70	0		●	Ten-GigabitEthernet0/0.4000	

图 6-164 物理链路

(2) 检查物理链路配置

“物理链路”的配置包括名称等诸多重要参数。物理链路的名称应尽量明确、便于理解。下一跳通常为 LB 三层直联对端设备的接口地址，与 Internet 互联链路的下一跳通常为 ISP 线路网关地址，与内网互联链路的下一跳通常为指向内网方向路由表项的下一跳地址。在检查下一跳时，应同时检查接口是否正确。物理链路的名称、下一跳信息不能编辑，如需修改可先将配置错误的物理链路删除后，重新创建一条物理链路。在 ISP 选项中，可设置物理链路对应的运营商类型，该功能必须在导入专用 ISP 地址表项文件后方可启用，具体操作方法不在本云图的讨论范围内。一般情况下，除带外管理端口外，LB 启用了多少个三层业务口，就应该配置多少条物理链路一一对应。对于连接 ISP 的物理链路，可启用健康性检测功能以实时探测线路状态，若健康性检查功能探测失败，说明该 ISP 线路可能存在故障，LB 将主动禁用该物理链路，将 DNS 解析调度至其他可用线路，同时还将向信息中心输出线路“Block”告警日志。健康性检测功能支持在单条物理链路上同时启用多种探测方法，通常设置为当其中任一种方法探测成功时即认为该线路正常，从而避免出现频繁的线路阻塞与恢复。对于 LB 与内网互联对应的物理链路，因其稳定性较好，推荐不启用健康性检测以减少探测流量。

例如：在 LB Web 管理界面“负载均衡→链路负载均衡→物理链路”中，单击“操作”列中

的“编辑”按钮，进入“修改物理链路”页面，对配置参数进行检查与修改，如图 6-165 所示。



图 6-165　修改物理链路

（3）检查健康性检测配置

LB 默认配置预定义了“icmp”“tcp_half_open”两种方法用于物理链路的健康性检测，启用后 LB 默认向该物理链路配置的“下一跳”地址进行探测。若网络管理员希望对远端跨网段的其他 IP 地址进行探测，可自定义检测方法并在物理链路配置中进行引用。若当前物理链路为失效状态，并且引用了自定义检测方法，那么就需要检查其配置是否正确、确认被检测 IP 是否能够响应 icmp、tcp_half_open 类型的探测报文。

例如：在 LB Web 管理界面“负载均衡→健康性检查”中，单击“操作”列中的“编辑”按钮，进入“修改健康性检查”页面，对配置参数进行检查与修改。在图 6-166 中，客户希望对 CTC 物理链路除下一跳地址外，对该线路相应的 DNS 服务器可达性做同步探测，服务器 IP 地址以 x. x. x. x 示意。

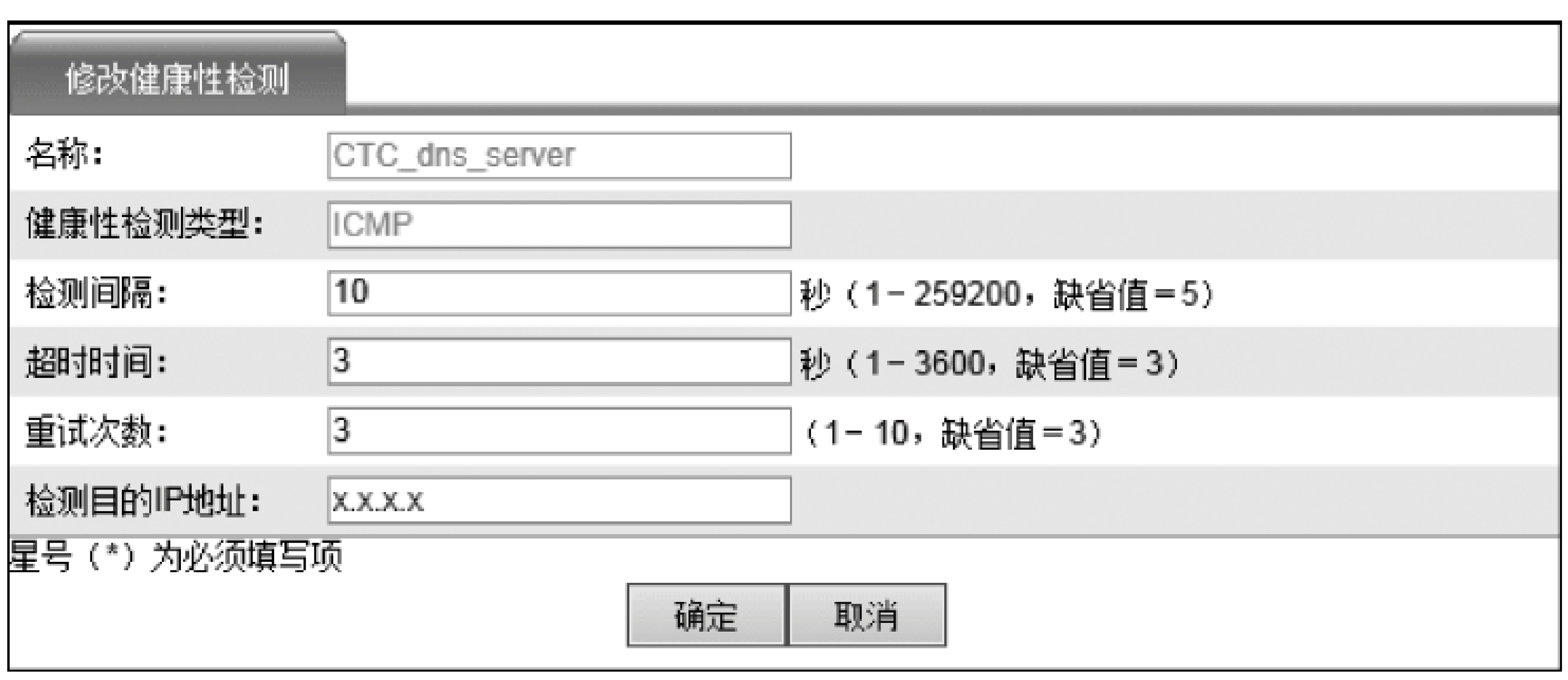


图 6-166　修改健康性检测

（4）检查物理线路可达性

查看 LB 设备的 ARP、路由表等网络可达性信息，通过 ping 测试等方法确认 LB 与其他网络设备互联互通正常。需注意：即使正常状态下业务流量是通过虚服务调度转发的，但依然要确保 LB 上正确学习了全部的网络可达性信息，比如为 LB 配置了完整的静态路由表。

命令：*display arp*

例如：在命令行界面查看 ARP 表项学习是否正确，IP 对应 MAC 地址是否正确。

```
[H3C] display arp
                 Type: S-Static    D-Dynamic
IP Address       MAC Address       VLAN ID   Interface              Aging Type
172.16.10.1      000f-e280-de93    N/A       XGE0/0.10              20    D
172.16.20.1      000f-e280-de93    N/A       XGE0/0.20              20    D
172.31.255.1     3ce5-a682-c521    N/A       XGE0/0.4000            20    D
```

（5）检查端口状态

检查 LB 各三层接口的速率、双工协商状态及对端状态是否正常，接口收发报文统计是否合理，是否存在错包，是否存在大量 TTL 超时报文（通常是路由环路造成）等。插卡形态的 LB 主要利用与宿主路由交换主机的内联万兆口承载业务流量，推荐采用三层子接口的部署方式。

命令：*display interface interface-type interface-number*

例如：在 CLI 界面查看 LB 插卡内联口状态。

```
<H3C>display interface Ten-GigabitEthernet 0/0
Ten-GigabitEthernet0/0 current state: Up
Line protocol current state: Up
Description: Ten-GigabitEthernet0/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 3ce5-a613-ff0c
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 3ce5-a613-ff0c
Media type is twisted pair, loopback not set, promiscuous mode not set
10Gb/s, Full-duplex, link type is force link
Output flow-control is disabled, input flow-control is disabled
Last clearing of counters: Never
    Peak value of input:20177 bytes/sec, at 2013-4-26 15:23:11
    Peak value of output: 19706 bytes/sec, at 2013-4-26 15:23:11
    Last 5 seconds input rate12994 bytes/sec, 103952 bits/sec, 127 packets/sec
    Last 5 seconds output rate 13015 bytes/sec, 104120 bits/sec, 127 packets/sec
    Input:136427 packets, 0 jumboes, 2742408 bytes, 136427 buffers
            6014 broadcasts, 4412 multicasts, 0 pauses
            0 errors, 0 runts, 0 giants
            0 crc, 0 align errors, 0 overruns
            0 dribbles, 0 drops, 0 no buffers
    Output:19822 packets, 2787464 bytes, 19822 buffers
            826 broadcasts, 0 multicasts, 0 pauses
            0 errors, 0 underruns, 0 collisions
            0 deferred, 0 drops, 0 lost carriers
```

（6）检查 DNS 重定向配置

在 Inbound 链路负载均衡中，目前 LB 可以支持 DNS A 记录、MX 记录的动态智能解析。在进行配置检查时，应重点查看“使能 DNS 重定向”选项是否已经启用。在成功导入 ISP 地址表项文件并设置物理链路 ISP 属性的前提下，建议启用“使能 ISP 选路”功能：源自不同运营商网络的本地 DNS 服务器或客户端，向 LB 发送 DNS 解析请求报文后，LB 可以直接根据 DNS 请求报文的源 IP 地址判断其所属运营商，并将对应物理链路上的“IP 地址”作为结果进行 DNS 解析应答。简而言之，电信用户返回电信线路地址，联通用户返回联通线路地址。在

“DNS 表项”页签中，需重点检查域名、IP 地址、物理链路等是否配置准确。需要根据 DNS 请求报文源 IP 地址强行指定应答结果的，可通过启用 ACL 策略实现。

Inbound 链路负载均衡中，设备将根据多种方式最终决定以哪个“IP 地址”作为 DNS 解析结果应答给客户端，优先顺序由高至低依次为：ACL 策略>ISP 选路>就近性>调度算法(随机)。当 LB 接收到来自运营商本地 DNS 服务器或客户端的 DNS 解析请求后，首先将报文源 IP 地址与 ACL 策略进行匹配，然后再与 ISP 地址表项进行匹配，如果前两者仍不能决定应答哪个 IP，就再与就近性表项进行匹配，仍然无法决定的，LB 将从该域名配置的多个 IP 中随机选择一个作为调度结果，应答客户端请求。应答后立即发起就近性探测，以尝试判断刚才的客户端地址从哪条物理链路可更快到达，建立就近性表项后用于后续 DNS 解析请求的决策。默认情况下，LB 应答的 DNS 解析结果有效时间为 60 秒。

例如：在负载均衡设备 Web 管理界面“负载均衡→链路负载均衡→Inbound”中，检查配置，如图 6-167 所示。

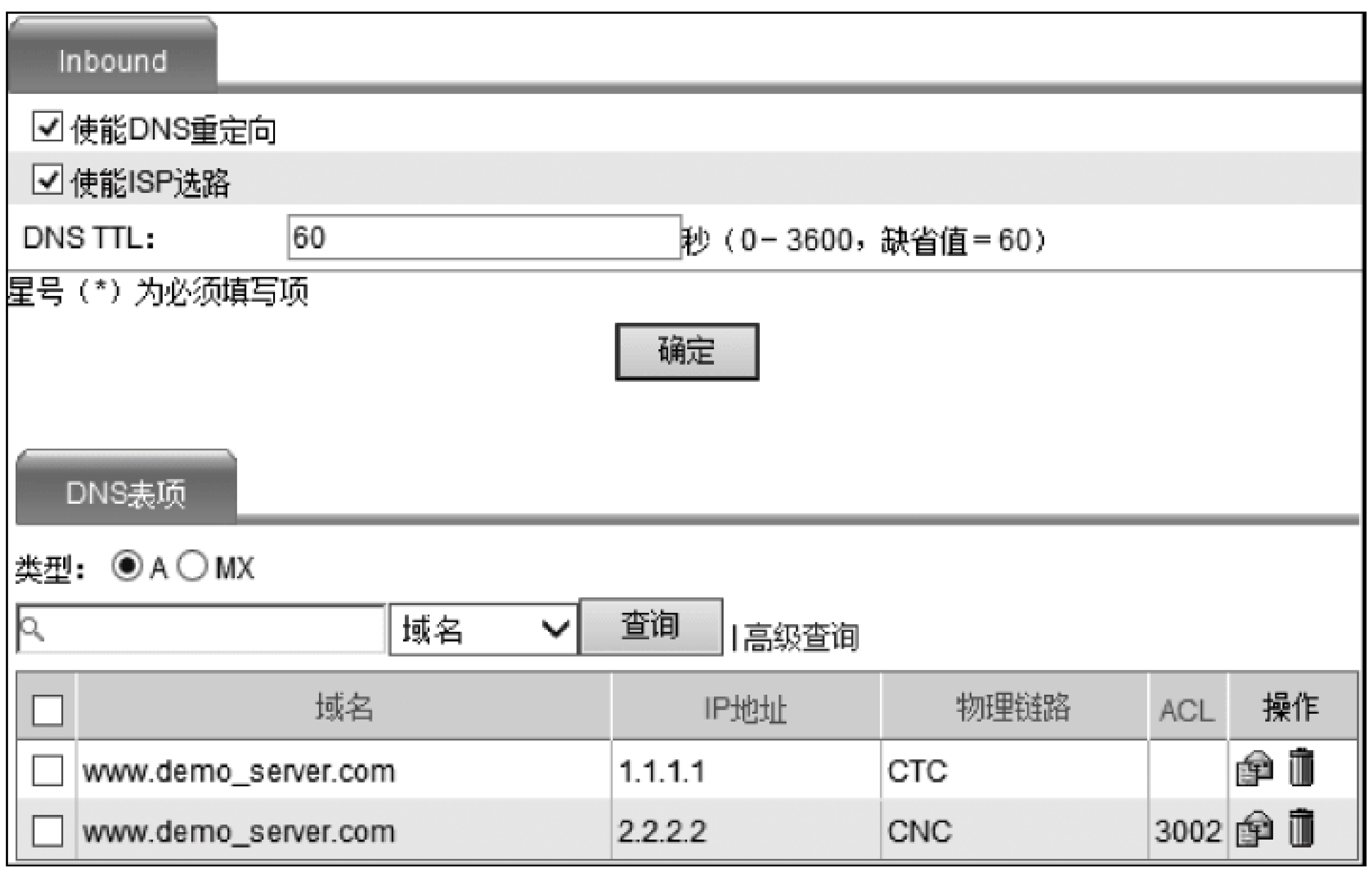


图 6-167　Inbound 配置

例如：若发现“DNS 表项”配置有误，可单击“操作”列中的“编辑”按钮，进入“修改 DNS 记录”页面，重新选择域名/IP 地址所对应的物理链中及关联的 ACL 规则，如图 6-168 所示。

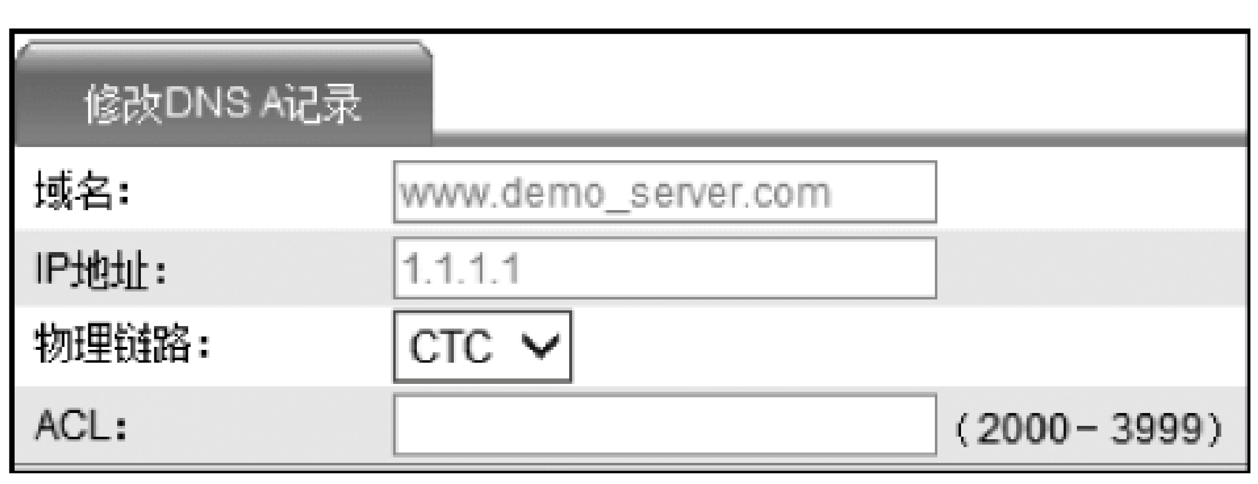


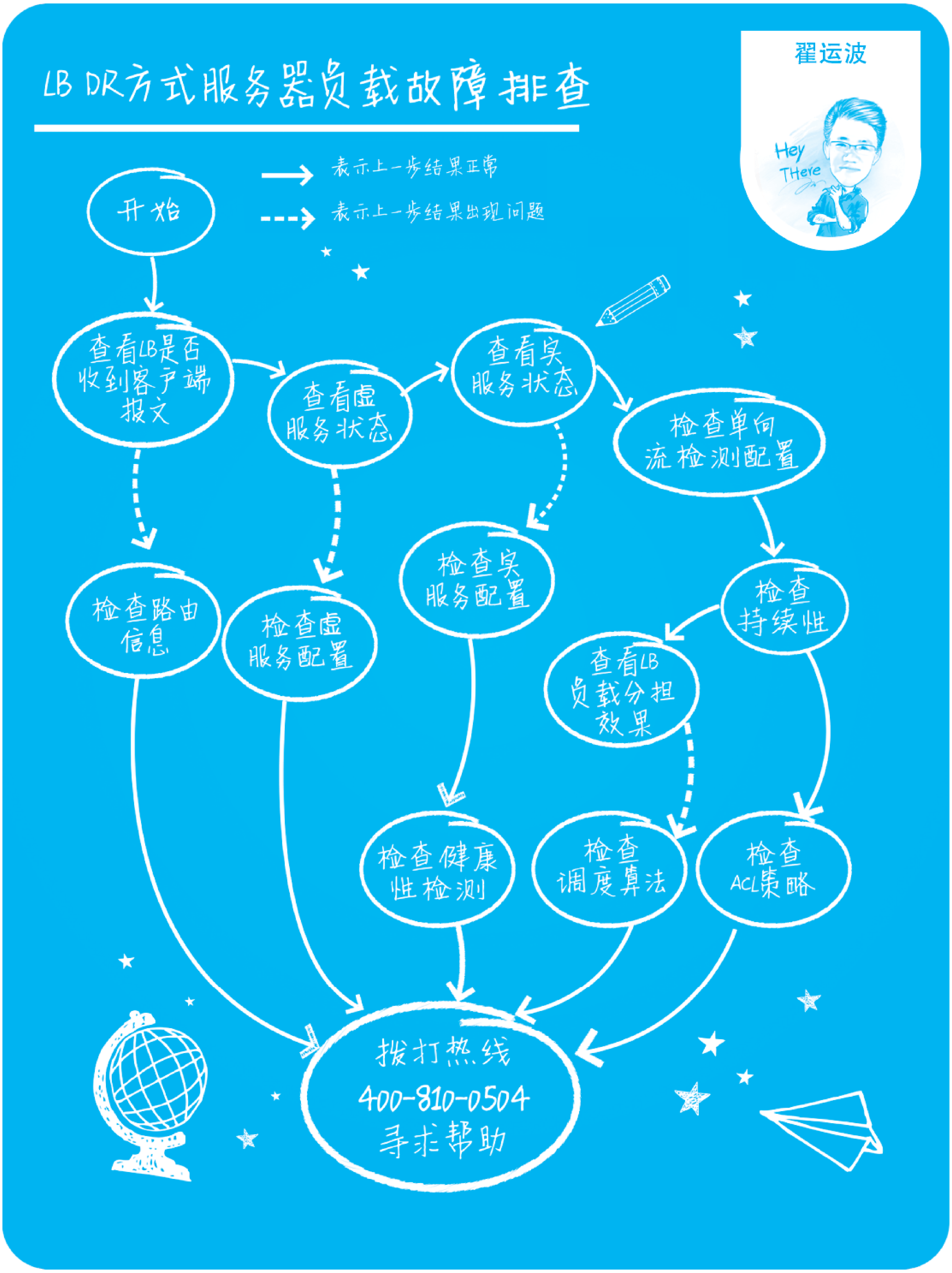
图 6-168　修改 DNSA 记录

(7) DNS 解析测试

在 Inbound 链路负载均衡中，LB 设备主要是面向 Internet 上的运营商本地 DNS 服务器或客户端提供动态 DNS 解析功能。须注意，LB 仅提供管理员明确配置的 A 记录、MX 记录解析。在一般场景中，需要原有域名注册服务商配合，将这些 DNS 记录的解析工作转移至 LB 完成，即“设法通知”Internet 上的运营商本地 DNS 服务器或客户端，对于这些 DNS 记录的解析请求，需直接向 LB(任意一个路由可达的接口)发起查询；对于超出 Inbound 负载均衡配置

的解析工作，LB 无法完成。在部分存在 NAT 的组网中，要注意 DNS 应答报文经过 NAT 设备时，NATT ALG 功能导致应答结果被修改的可能。

最简单的验证方法：将测试 PC 客户端的主用 DNS 服务器设备为 LB 设备任意一个路由可达的接口地址，然后在客户端上执行 DNS 请求操作，通过观察解析结果来判断 LB 是否正常。若客户端直接向 LB 请求，可以正确获取对应的 IP，说明 LB 设备本身工作正常；但如果将客户端的 DNS 重新设置为 Internet 运营商提供的本地 DNS 服务器后，发现仍然无法成功解析，则很可能是由于运营商本地 DNS 服务器、原域名注册服务器等配合存在问题，未能使运营商本地 DNS 服务器向 LB 直接发起 DNS 解析请求导致。



LB DR方式服务器负载故障排查
翟运波
Hey THere
表示上一步结果正常
表示上一步结果出现问题
开始
查看LB是否收到客户端报文
查看虚服务状态
查看真服务状态
检查单向流检测配置
检查路由信息
检查虚服务配置
检查真服务配置
检查持续性
查看LB负载分担效果
检查健康性检测
检查调度算法
检查ACL策略
拨打热线
400-810-0504
寻求帮助

1. 开始

DR(Direct Routing)方式服务器负载均衡技术通过改写报文的目的 MAC 地址实现,对负载均衡设备和服务器的组网有一定要求,DR 方式服务器负载定位故障的思路是:先确认 LB 是否收到客户请求报文,其次检查虚服务和实服务状态,然后检查单向流检测配置,再检查调度算法,最后检查持续性和 ACL 策略。

2. 流程图相关操作说明

(1) 查看 LB 是否收到客户端报文

LB 将不同客户的请求分发给不同的服务器,从而实现负载分担的目的,所以定位问题时首先要判断 LB 是否收到客户端的请求报文,具体可以通过在 LB 上查看会话或者抓包的方法进行确认,另外 DR 方式中服务器返回的报文不用经过 LB,所以查看会话的时候响应方收到的报文应该是 0。

命令: *display session table source-ip x.x.x.x destination-ip y.y.y.y verbose*

例如:通过命令可以发现 LB 已经收到客户端 10.0.0.1 发来的请求报文。

```
[H3C]display session table source-ip 10.0.0.1 destination-ip 60.191.99.142 verbose
Initiator:
  Source IP/Port : 10.0.0.1/53047
  Dest IP/Port   : 60.191.99.142/80
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 60.191.99.142/80
  Dest IP/Port   : 10.0.0.1/53047
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)       App: HTTP               State: TCP-EST
Start time: 2013-09-08 18:10:49   TTL: 3599s
Root                          Zone(in):
                              Zone(out):
Received packet(s)(Init): 9 packet(s) 9310 byte(s)
Received packet(s)(Reply): 0 packet(s) 0 byte(s)
```

(2) 检查路由信息

如果通过查看会话或者抓包发现 LB 没有收到客户的请求报文,那么需要对路由进行排查,确保上行设备都有到达 LB 的虚服务 IP 地址的路由。

命令: *display ip routing-table x.x.x.x*

例如:LB 的虚地址是 60.191.99.142,通过命令看到上行设备已经有到 60.191.99.142 的路由。

```
<SW>display ip routing-table
Routing Tables: Public
        Destinations : 9        Routes : 9

Destination/Mask    Proto  Pre  Cost        NextHop        Interface

10.0.0.0/24          Direct 0    0           10.0.0.254      Vlan10
```

```
10.0.0.254/32      Direct 0    0          127.0.0.1       InLoop0
20.0.0.0/24        Direct 0    0          20.0.0.1        Vlan20
20.0.0.1/32        Direct 0    0          127.0.0.1       InLoop0
60.191.99.142/32   Static 60   0          20.0.0.2        Vlan20
...
```

另外,加入 LB 的虚服务 IP 地址和接口地址在同一物理网段,由于 LB 的虚地址目前不会响应 ARP,所以需要在上行设备配置 32 位主机路由,或者将 LB 虚地址配置成接口 sub 地址或 VRRP 虚地址。

例如:LB 的接口地址为 20.0.0.0/24,虚服务 IP 地址是 20.0.0.100,可以将虚服务地址配置成接口 sub 地址或者 VRRP 虚地址。

```
[H3C]display current-configuration interface Ten-GigabitEthernet 0/0.20
#
interface Ten-GigabitEthernet0/0.20
 vlan-type dot1q vid 20
 ip address 20.0.0.2 255.255.255.0
 ip address 20.0.0.100 255.255.255.0 sub
#
[H3C]display current-configuration interface Ten-GigabitEthernet 0/0.20
#
interface Ten-GigabitEthernet0/0.20
 vlan-type dot1q vid 20
 ip address 20.0.0.2 255.255.255.0
 vrrp vrid 20 virtual-ip 20.0.0.100
 vrrp vrid 20 priority 120
#
```

(3) 查看虚服务状态

登录到 LB 设备的 Web 管理界面,查看 LB 虚服务的状态是否正常,如果虚服务没有使能或者虚服务对应的所有实服务都出现异常,则虚服务会显示红灯,LB 不会对命中虚服务的报文进行转发,所以一定要检查配置,确认虚服务已经使能,且状态显示为绿灯。

例如:进入 LB 的 Web 管理界面,在导航栏中单击"负载均衡"→"服务器负载均衡"→"IPv4 协议",单击"虚服务"页签,如图 6-169 所示,可以看到当前 LB 上 http_service 的虚服务状态正常,但是 dns_service 这个虚服务的状态不正常。



图 6-169　虚服务

(4) 检查虚服务配置

如果虚服务的状态不正常,请仔细检查虚服务是否已经使能,然后检查虚服务的 IP 地址、掩码、协议和端口是否配置正确。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“虚服务”页签，然后单击对应虚服务后面的编辑按钮进入虚服务的配置界面，如图 6-170 和图 6-171 所示可以看到 http_service 这个虚服务的 IP 地址、掩码、协议及端口信息配置正确，并确认虚服务状态已经使能。



图 6-170 虚服务配置



图 6-171 修改虚服务

(5) 查看实服务状态

LB 通过健康性检测实时监控各实服务的状态，状态正常的实服务显示绿灯，一旦检测到实服务故障，就显示红灯。LB 不会向故障的实服务分发流量，在日常维护过程中要及时关注实服务的状态。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“实服务”页签，如图 6-172 所示，可以看到 httpserver1 和 httpserver2 的健康性检测状态正常，dnsserver1 和 dnsserver2 的状态不正常。

(6) 检查实服务配置

如果实服务的状态不正常，需要检查实服务的 IP 地址、端口以及健康性检测类型等配置。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“实服务”页签，然后单击对应实服务后面的编辑按钮进入实服务的配置界面，如图 6-173 和图 6-174 所示，看到实服务 httpserver1 的 IP 地址、端口配置正确，健康性检测方法和实服务组一致。



图 6-172　实服务



图 6-173　实服务配置

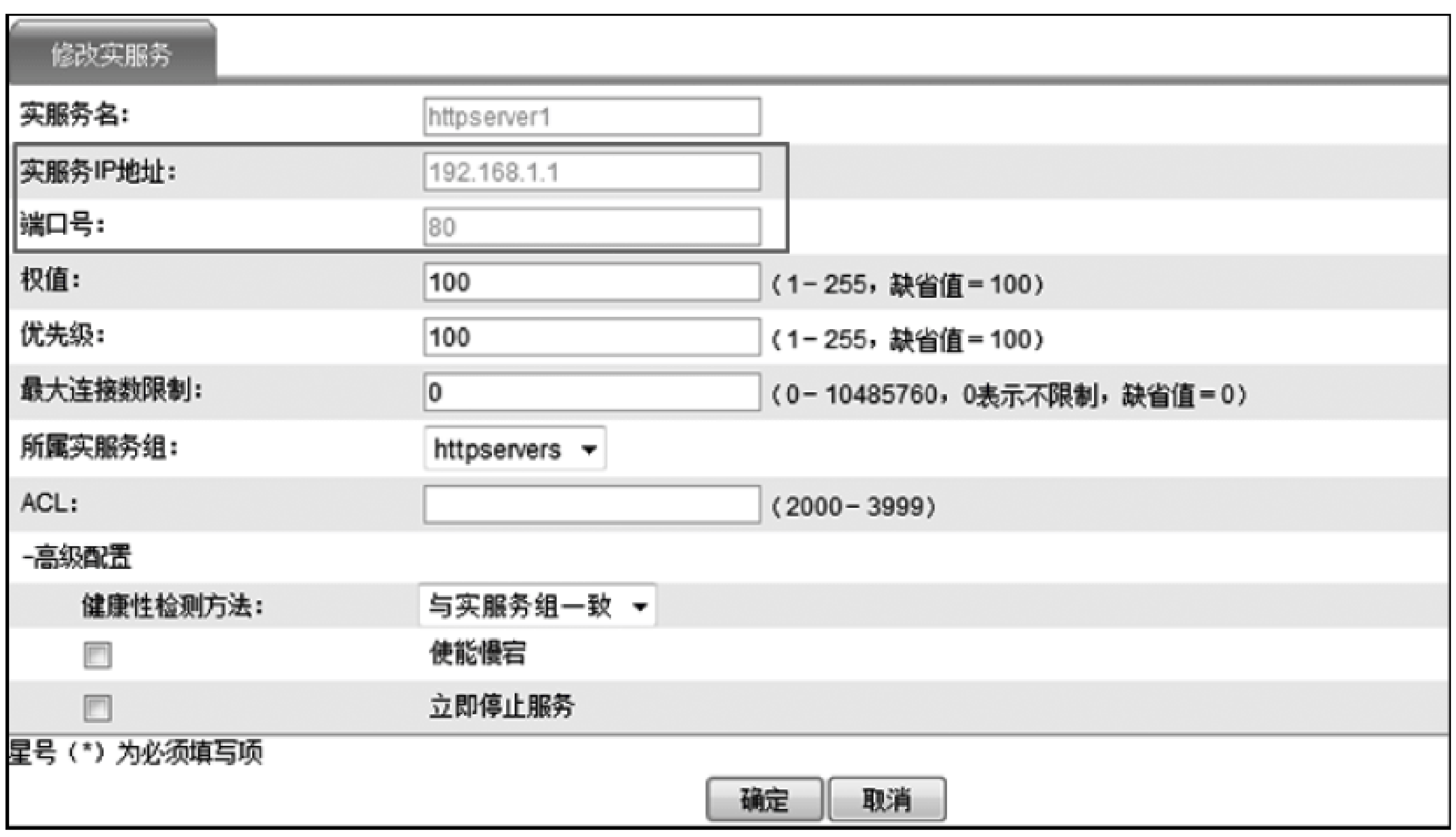


图 6-174　修改实服务

(7) 检查健康性检测

LB 通过健康性检测实时监控实服务的状态，如果实服务出现异常就显示红灯，并且会输出日志提示，当实服务出现异常的时候除了检查实服务的 IP 地址、端口等配置是否正确外，还应该及时根据实服务的健康性检测类型检查实服务的路由可达性、实服务提供业务的端口、进程或者应用程序是否正常。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“实服务”页签，然后单击对应实服务后面的编辑按钮进入实服务的配置界面，如图 6-175 所示看到 httpserver1 这个实服务的健康性检查选择的类型和实服务组一致，再单击“实服务组”页签，查看实服务组的健康性检测类型是 ICMP 如图 6-176 所示，然后进入

LB 的健康性检测配置页面检查 ICMP 的相关配置参数，如图 6-177 所示。ICMP 主要用于检测服务的可达性，通过命令可以看到 LB 到实服务 192.168.1.1 的路由正常。



图 6-175　修改实服务

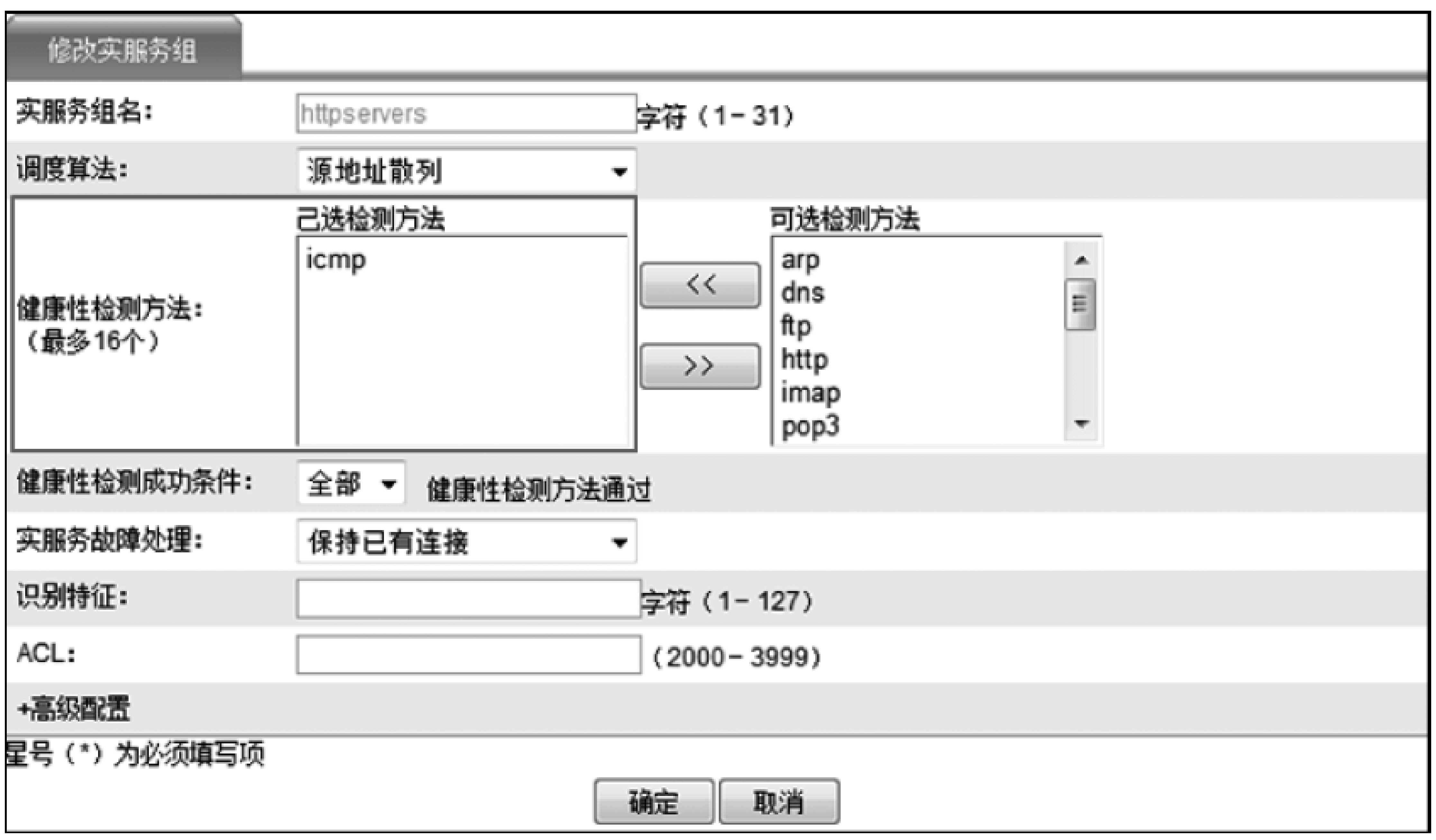


图 6-176　修改实服务组



图 6-177　修改健康性检测

```
<LB>display ip routing-table 192.168.1.1
Routing Table : Public
Summary Count : 1
Destination/Mask     Proto   Pre   Cost        NextHop         Interface
192.168.1.0/24       Direct  0     0           192.168.1.254   XGE0/0.50

<LB>ping 192.168.1.1
  PING 192.168.1.1: 56   data bytes, press CTRL_C to break
    Reply from 192.168.1.1: bytes=56 Sequence=0 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms

  --- 192.168.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

(8) 检查单向流检测配置

LB 的 DR 方式负载分担模式中，只有客户端的请求报文经过 LB，服务器响应的报文不会经过 LB，也就是只有单方向的报文经过 LB，为了保证会话的正常建立，LB 需要开启“单向流检测”功能。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“安全特性”→“会话管理”→“基本设置”，选中“流检测”下面的“启用单向流检测”复选框，如图 6-178 所示。

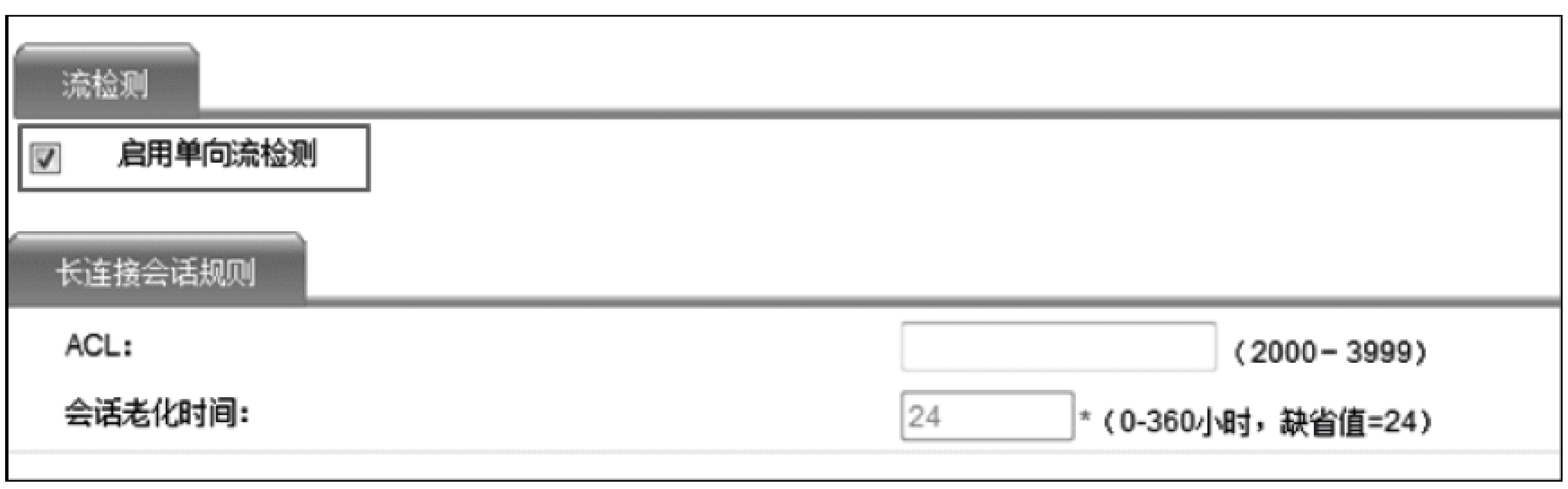


图 6-178 流检测

(9) 查看 LB 负载分担效果

LB 提供了丰富的统计功能，可以对每个虚服务、实服务的连接数、连接速率、收发报文数等信息进行统计，通过统计信息可以看到 LB 当前的负载分担效果。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，单击“统计信息”页签，如图 6-179 所示，可以查看虚服务 http_service 及其关联实服务 httpserver1 和 httpserver2 的总连接数、连接速率等信息，从当前统计情况来看，httpserver1 和 httpserver2 的负载效果非常均匀。

(10) 检查调度算法

如果通过虚服务的统计信息看到服务器负载的效果不均匀，应该及时根据业务情况调整

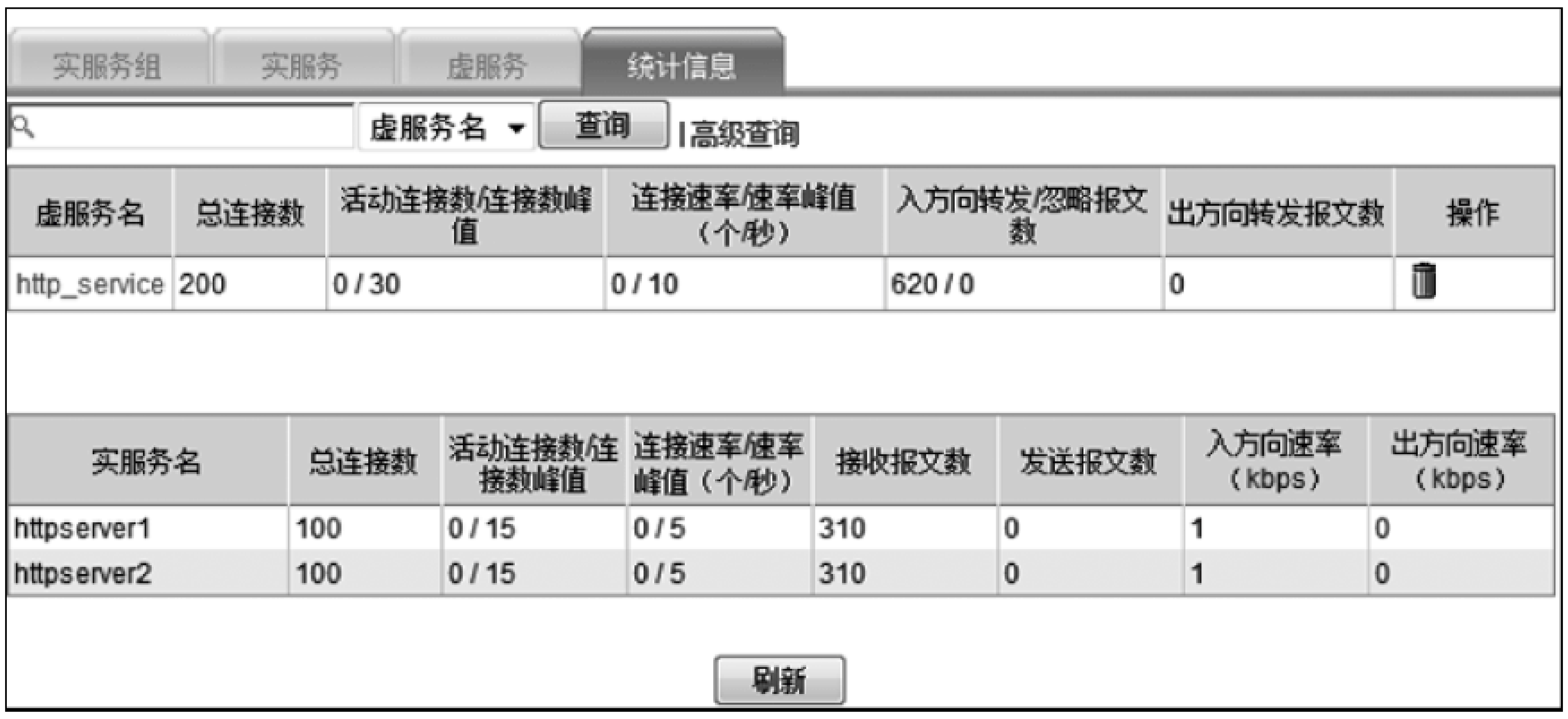


图 6-179　统计信息

调度算法。调整的时候先找到对应的虚服务，然后查看虚服务关联的是服务组，修改该实服务组的调度算法。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“虚服务”页签，如图 6-180 所示查看 http_service 关联的实服务组是 httpservers，然后进入 httpservers 实服务组的配置界面调整其调度算法，如图 6-181 所示。



图 6-180　虚服务



图 6-181　修改实服务组

(11) 检查持续性

持续性就是在一定时间内将多个具有相同特性或者相关特性的连接持续发送到同一个服务器，LB 支持基于源 IP、源端口、目的 IP、目的端口等多方式的持续性，使能持续性功能后，LB 会生成一张持续性表项，排错问题的时候先检查持续性表项是否正确，如果不正确需要及时调整持续性配置。

命令：*display load-balance persistence server vd-name root virtual-service xxxx*

例如：通过命令可以看到 LB 已经生产基于源 IP 的持续性表项，源 IP 是 10.0.0.1，对应的实服务是 192.168.1.2，表项的老化时间是 600 秒，当前连接数有 20 个。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]_h
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]display load-balance persistence server vd-name root virtual-service http_service
 Persistence method : Source-IP binding
 Source-IP              Real-Server IP     Conn-Num          Age
 10.0.0.1               192.168.1.2          20              600
[H3C-hidecmd]quit
```

如果持续性表项无法生成或者不正确，请登录到 LB 的 Web 管理界面检查持续性的配置是否正确。

例如：进入 LB 的 Web 管理界面，在导航栏中单击“负载均衡”→“服务器负载均衡”→“IPv4 协议”，先单击“虚服务”页签，然后单击 http_service 虚服务后面的编辑按钮进入虚服务配置界面，可以看到持续性选择了“源地址方式”，持续性表项生命值是 600 秒，如图 6-182 所示。

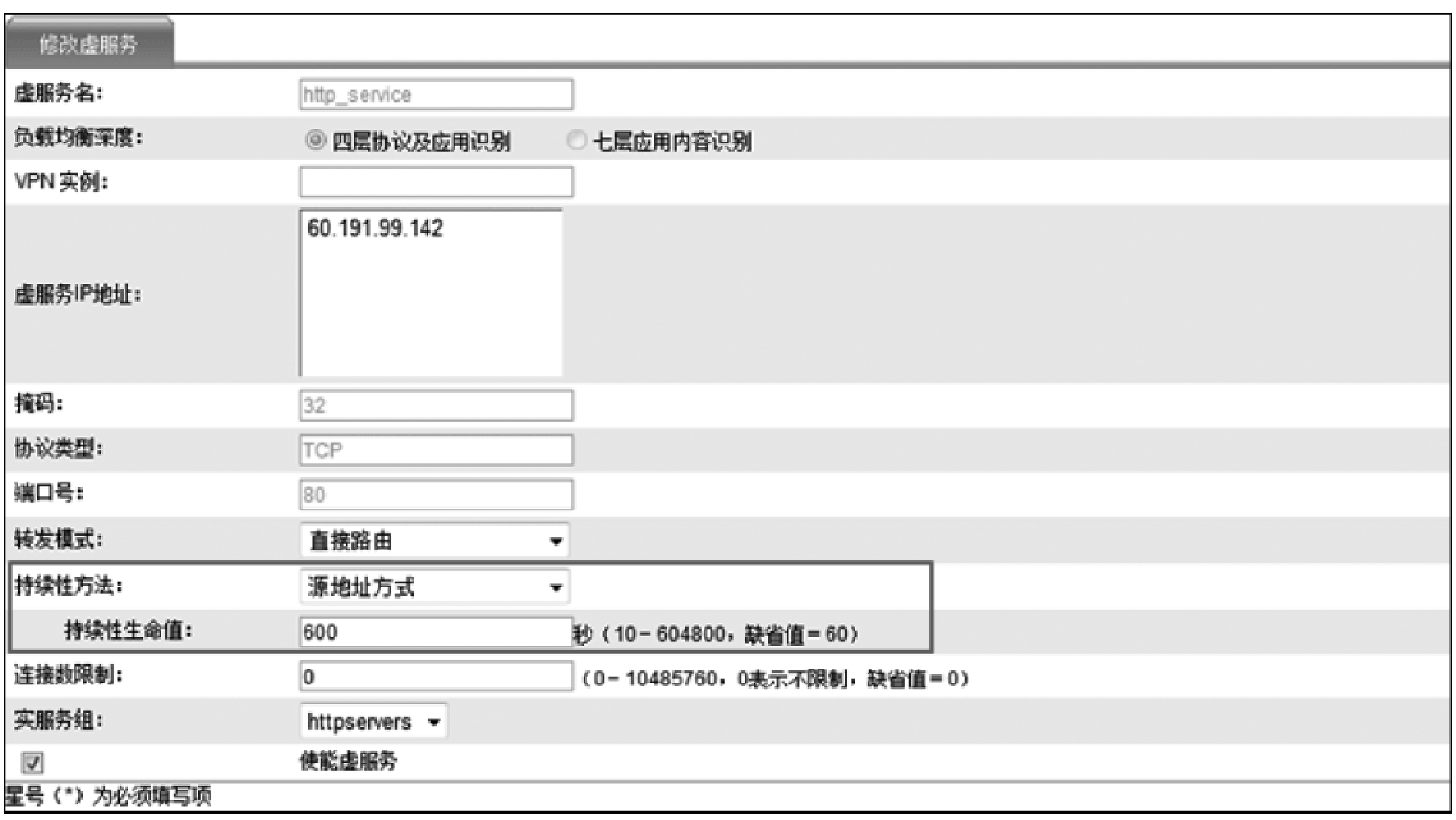


图 6-182　修改虚服务

(12) 检查 ACL 策略

在某些应用场景下,客户要求将某些特点的数据流分发给特定的服务器,在 LB 上可以通过 ACL 策略来实现,在排查的过程中可以通过会话来查看 ACL 策略是否生效,如果不生效需要仔细检查 ACL 策略的配置。

命令:*display acl xxxx*

例如:客户要求将来自 10.0.0.10 的所有流量分发给 192.168.1.1 这台实服务,命令行下面创建了一个 ACL 3001,定义需要转发的流量,然后在 LB Web 管理界面将 ACL 3001 关联到 192.168.1.1 这台实服务,如图 6-183 所示。

```
[H3C]display acl 3001
Advanced ACL  3001, named -none-, 1 rule,
ACL's step is 5
 rule 0 permit ip source 10.0.0.10 0 (20 times matched)
```

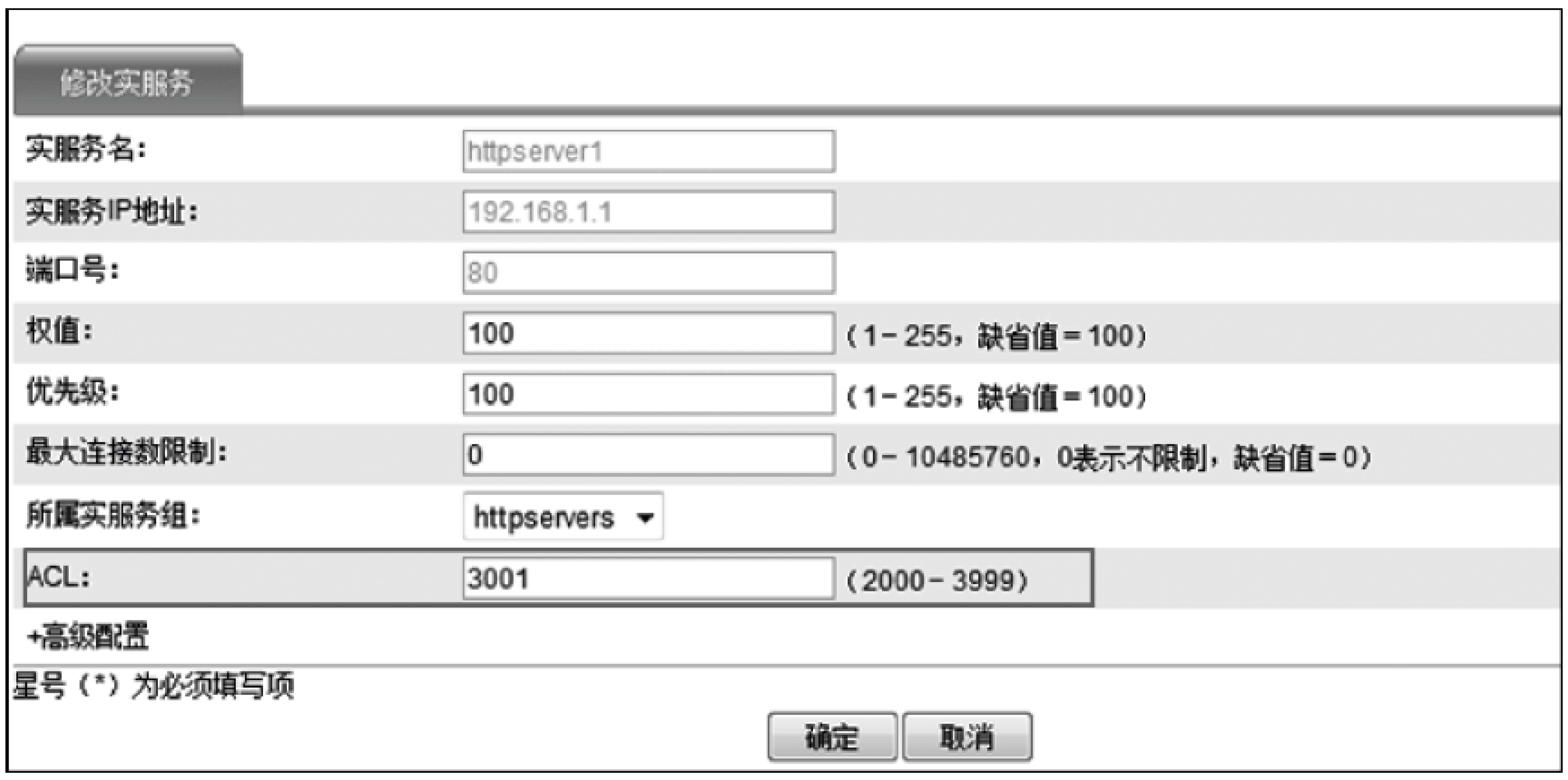
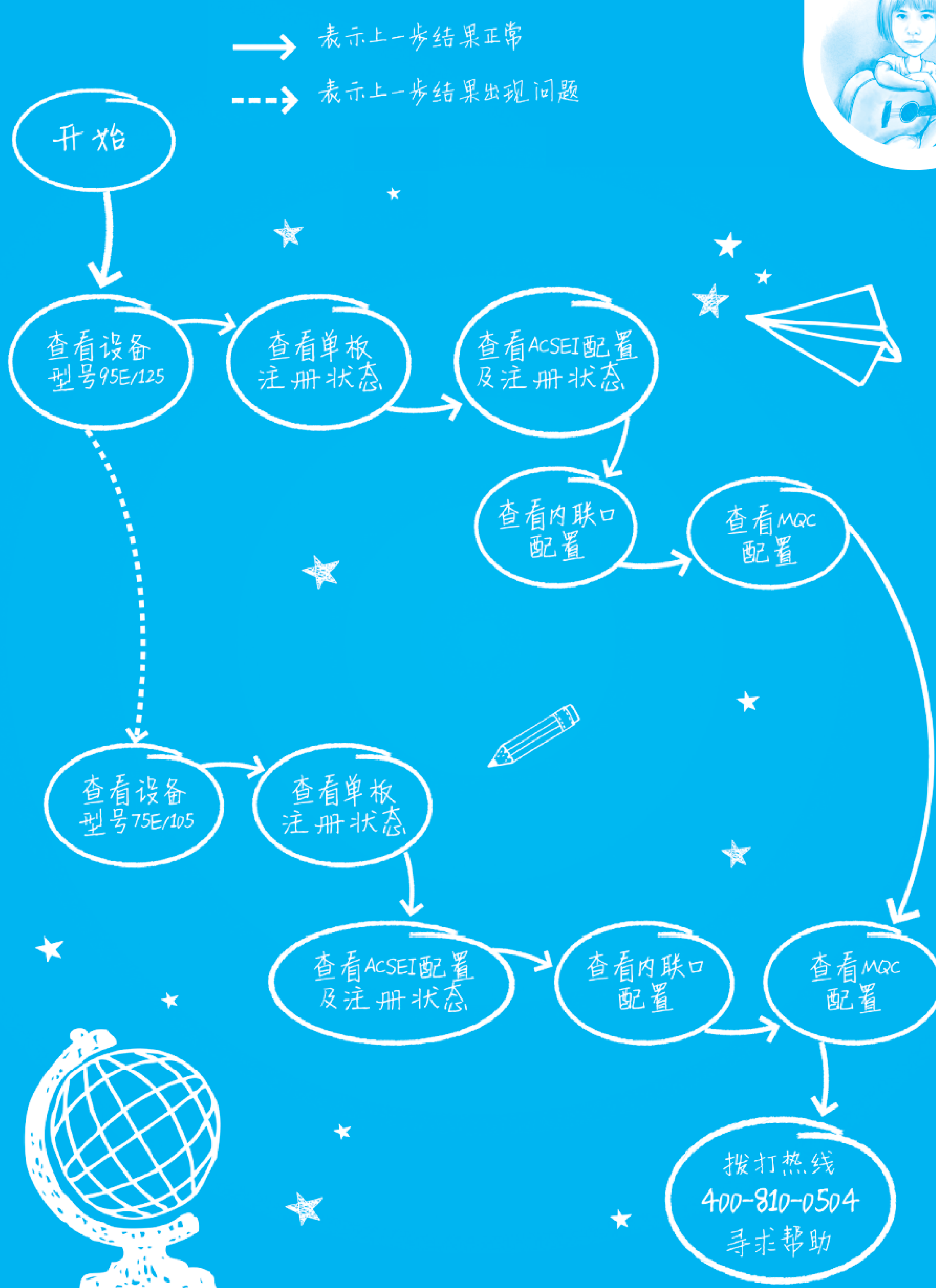


图 6-183　修改实服务

IPS(ACG)MQC引流问题故障排查





1. 开始

MQC 技术主要用于二层插卡的引流。在堆叠或者其他无法使用 OAA 的情况下,往往需要通过配置 MQC 来进行引流工作,将需要经过 IPS/ACG 处理的报文定向到二层板卡。

MQC 引流问题定位故障的思路是:参考配置进行一步步的排查,查看单板注册状态,内联口配置以及 MQC 具体配置等。

2. 流程图相关操作说明

(1) 查看设备型号 95E/125

通过登录交换机设备,查看交换机版本,确认交换机型号。

命令:*display version*

举例:通过命令查看当前交换机型号及版本,此设备是 125 系列交换机。

```
<H3C>display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 1828P03
Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S12508 uptime is 6 weeks, 6 days, 11 hours, 49 minutes
Last reboot reason : Power on

LST1MRPNC1 0:   uptime is 6 weeks, 6 days, 11 hours, 49 minutes
Last reboot reason : Power on
3456     Mbytes SDRAM
1024     Kbytes NVRAM Memory
Type       : LST1MRPNC1
BootRom    : 1.22
Software   : S12500-CMW520-R1828P03
Patch      : NONE
PCB        : Ver.B
```

(2) 查看单板注册状态

确认了现场设备为 95E/125 后,查看板卡在交换机的注册状态。

命令:*display device*

例如:通过命令查看,可以确认单板已经成功注册。

```
<H3C>display device
Slot No.   Brd Type        Brd Status    Software Version
 0         LST1MRPNC1      Master        S12500-CMW520-R1828P03
 1         NONE            Absent        NONE
 2         LST1GT48LEC1    Normal        S12500-CMW520-R1828P03
 3         LST1IPS1A1      Normal        S12500-CMW520-R1828P03
 4         LST1ACG1A1      Normal        S12500-CMW520-R1828P03
 5         LST1FW2A1       Normal        S12500-CMW520-R1828P03
 6         LST1LB1A1       Normal        S12500-CMW520-R1828P03
 7         NONE            Absent        NONE
 8         NONE            Absent        NONE
 9         NONE            Absent        NONE
 …
```

如果单板注册失败，为 fault 状态，请联系 400 处理。

(3) 查看 ACSEI 配置及注册状态

查看交换机上 ACSEI 配置及注册状态，同时确认 IPS/ACG 上 ACFP CLIENT 是否使能。

命令：*display current-configuration* | *include acsei*

　　　display acsei client info

例如：通过命令查看，可以确认交换机使能 acsei server。

```
<H3C>display current-configuration | include acsei
 acsei server enable
```

通过命令查看，还可以确认单板已经成功完成 acsei 注册。

```
<H3C>display acsei client info
 Total Client Number: 1

 Client ID: 2
 Client Description: Application Control Gateway
 Hardware: 3.0
 System Software: i-Ware software, Version 1.10
 Application Software: Ess 6119P03
 CPU: RMI XLR732
 PCB Version: Ver.A
 CPLD Version: 3.0
 Bootrom Version: 1.19
 Storage Card: 247MB
 Memory: 3536MB
 Harddisk: 0MB
```

通过查看 Web 页面，确认 IPS/ACG 板卡 ACFP Client 是不是使能状态，如图 6-184 所示。

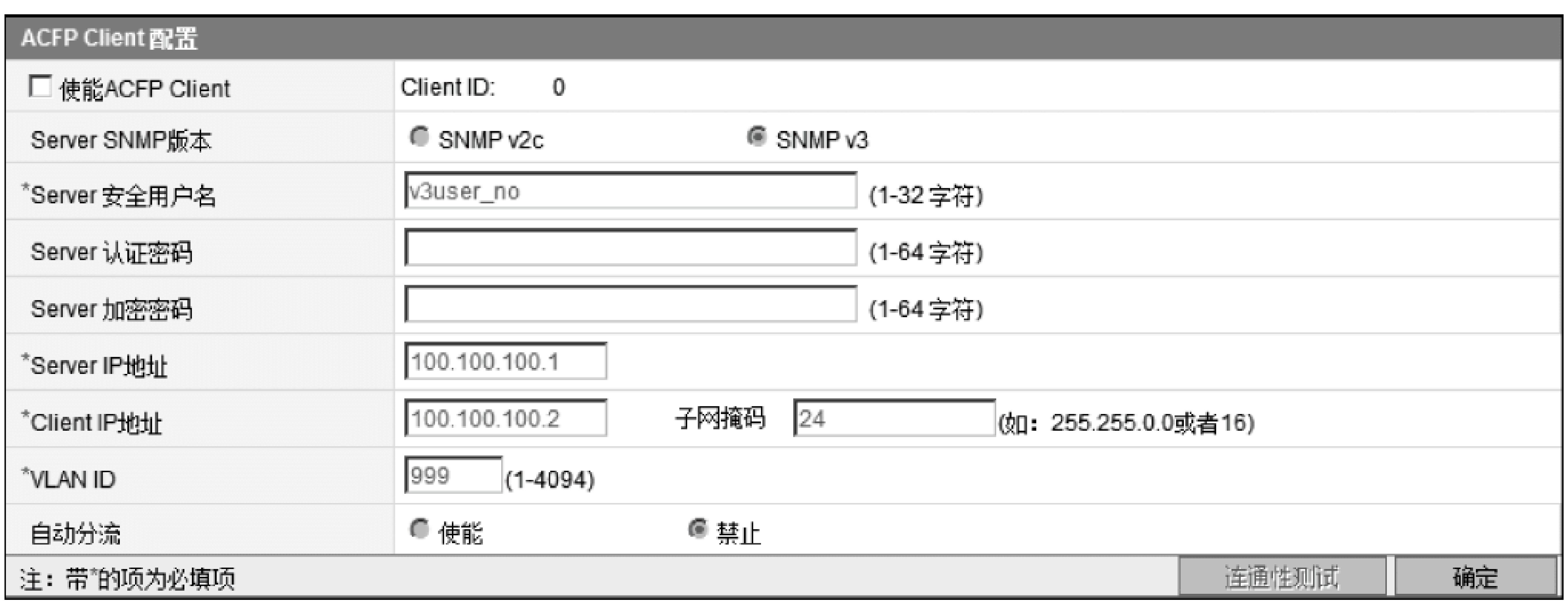


图 6-184　ACFP Client 配置

如果单板未成功注册 acsei，确认内联口未 shutdown 后，请联系 400 处理。

(4) 查看内联口配置

查看交换机内联口配置，是否放通了业务 VLAN 同时下发了防环路 ACL。

命令：*display current-configuration* | *begin* (*interface xxx*)

　　　display acl xxx

例如：通过查看内联口配置，确认内联口放通了业务 VLAN，同时配置了过滤策略。

```
<H3C>display current-configuration | begin (interface Ten-GigabitEthernet4/0/1)
#
interface Ten-GigabitEthernet4/0/1
 port link-mode bridge
 description to_ACG
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 stp disable
 packet-filter 4000 outbound
 packet-filter 4000 inbound
 mac-address max-mac-count 0
```

port trunk permit vlan 10 20 表示放通业务 VLAN；stp disable 表示关闭此接口生成树协议；packet-filter 4000 outbound 表示出方向过滤非业务报文；packet-filter 4000 inbound 表示入方向过滤非业务报文；mac-address max-mac-count 0 表示关闭 MAC 地址学习功能。

通过查看 ACL，确认过滤规则的配置。

```
<H3C>display acl 4000
Ethernet frame ACL  4000, named -none-, 3 rules,
filter
ACL's step is 5
 rule 0 permit type 0800 ffff dest-mac 0cda-41b6-41d8 ffff-ffff-ffff
 rule 50 permit type 88a7 ffff
 rule 100 deny
```

rule 0 permit type 0800 ffff dest-mac 0cda-41b6-41d8 ffff-ffff-ffff 表示放通业务报文；rule 50 permit type 88a7 ffff 表示放通 ACSEI 注册报文；rule 100 deny 表示拒绝非业务报文。

（5）查看 MQC 配置

查看交接口下 MQC 配置，确认配置正确下发，同时与 IPS/ACG 上安全域配置相匹配。

命令：*display qos policy interface xxx*

display acl xxx

例如：通过查看接口下 QoS 配置，确认引流规则正确下发。

```
<H3C>display qos policy interface GigabitEthernet 2/0/2

  Interface: GigabitEthernet2/0/2

  Direction: Inbound

  Policy: up_ACG
   Classifier: up_ACG
     Operator: AND
               Rule(s) : If-match service-vlan-id 10
               If-match destination-mac 0cda-41b6-41d8
               If-match acl 3001
     Behavior: up_ACG
      Redirect enable:
        Redirect type: interface
        Redirect destination: Ten-GigabitEthernet4/0/1
```

Redirect destination：Ten-GigabitEthernet4/0/1 表示重定向目的接口。

通过查看 ACL 配置，确认引流地址正确。

```
<H3C>dis acl 3001
Advanced ACL  3001, named -none-, 1 rule,
Match-ALL-Address-Up
ACL's step is 5
 rule 5 permit ip source 10.0.0.0 0.0.0.255
```

rule 5 permit ip source 10.0.0.0 0.0.0.255 表示匹配业务地址网段。

查看 IPS/ACG 插卡上安全区域配置，确认配置匹配，如图 6-185 所示。

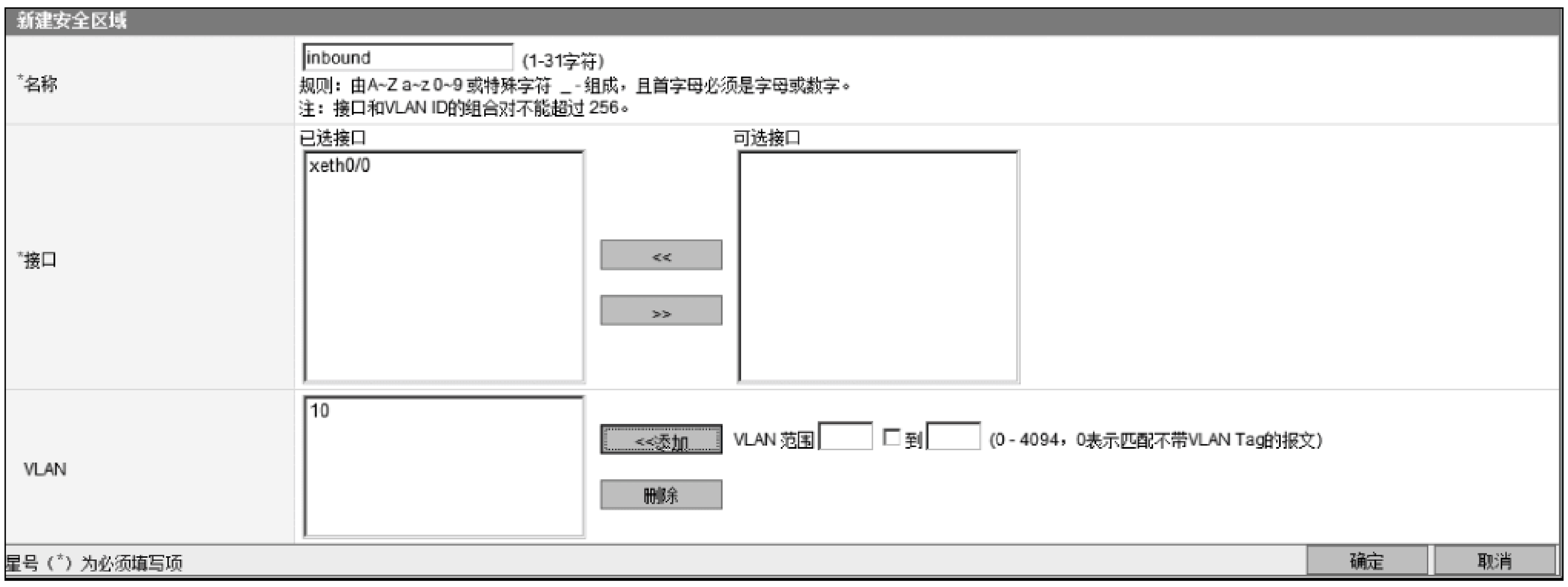


图 6-185　新建安全区域

查看 IPS/ACG 插卡上段配置，确认配置正确，如图 6-186 所示。

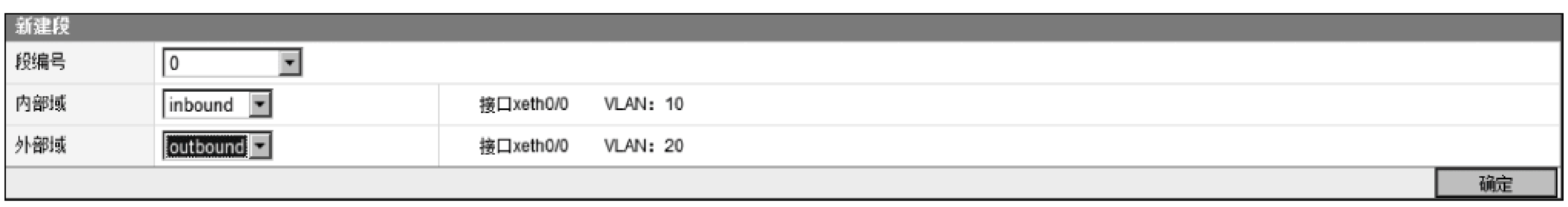


图 6-186　新建段

（6）查看设备型号 75E/105

通过登录交换机设备，查看交换机版本，确认交换机型号。

命令：*display version*

例如：通过命令查看当前交换机型号及版本。

```
[H3C]dis version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 6708P08
Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S7506E uptime is 1 week, 6 days, 16 hours, 35 minutes

MPU(M) 0:
Uptime is 1 weeks,6 days,16 hours,35 minutes
H3C S7506E MPU(M) with 1 BCM1125H Processor
```

```
BOARD TYPE:          LSQ1SRP2XB
DRAM:                512M bytes
FLASH:               64M bytes
NVRAM:               512K bytes
PCB 1 Version:       VER.B
PCB 2 Version:       VER.B
Bootrom Version:     303
CPLD 1 Version:      006
CPLD 2 Version:      006
Release Version:     H3C S7506E-6708P08
Patch Version:       None
```

(7) 查看单板注册状态

确认了现场设备为75E/105后，查看板卡在交换机的注册状态。

命令：*display device*

例如：通过命令查看，可以确认单板已经成功注册。

```
[H3C]dis device
Slot No. Brd Type      Brd Status  Subslot Num  Sft Ver          Patch Ver
 0       LSQ1SRP2XB    Master      0            S7500E-6708P08   None
 1       NONE          Absent      0            NONE             None
 2       LSQ1LBSC      Normal      0            S7500E-6708P08   None
 3       LSQ1IPSSC     Normal      0            S7500E-6708P08   None
 4       LSQ1LBSC      Normal      0            S7500E-6708P08   None
 5       LSQ1ACGASC    Normal      0            S7500E-6708P08   None
 6       LSQ1NSMSC     Normal      0            S7500E-6708P08   None
 7       LSU1GP24TXEB  Normal      0            S7500E-6708P08   None
 8       SRP2XBSLAVE   Normal      0            S7500E-6708P08   None
 9       NONE          Absent      0            NONE             None
```

如果单板注册失败，为fault状态，请联系400处理。

(8) 查看ACSEI配置及注册状态

查看交换机上ACSEI配置及注册状态，同时确认IPS/ACG上ACFP CLIENT是否使能。

命令：*display current-configuration | include acsei*

display acsei client info

例如：通过命令查看，可以确认交换机使能acsei server。

```
<H3C>display current-configuration | include acsei
 acsei server enable
```

通过命令查看，可以确认单板已经成功完成acsei注册。

```
<H3C>display acsei client info
 Total Client Number: 1

 Client ID: 2
 Client Description: Application Control Gateway
```

```
Hardware: 3.0
 System Software: i-Ware software, Version 1.10
 Application Software: Ess 6119P03
 CPU: RMI XLR732
 PCB Version: Ver. A
 CPLD Version: 3.0
 Bootrom Version: 1.19
 Storage Card: 247MB
 Memory: 3536MB
 Harddisk: 0MB
```

通过查看 Web 页面，确认 IPS/ACG 板卡 ACFP Client 是不是使能状态，如图 6-187 所示。

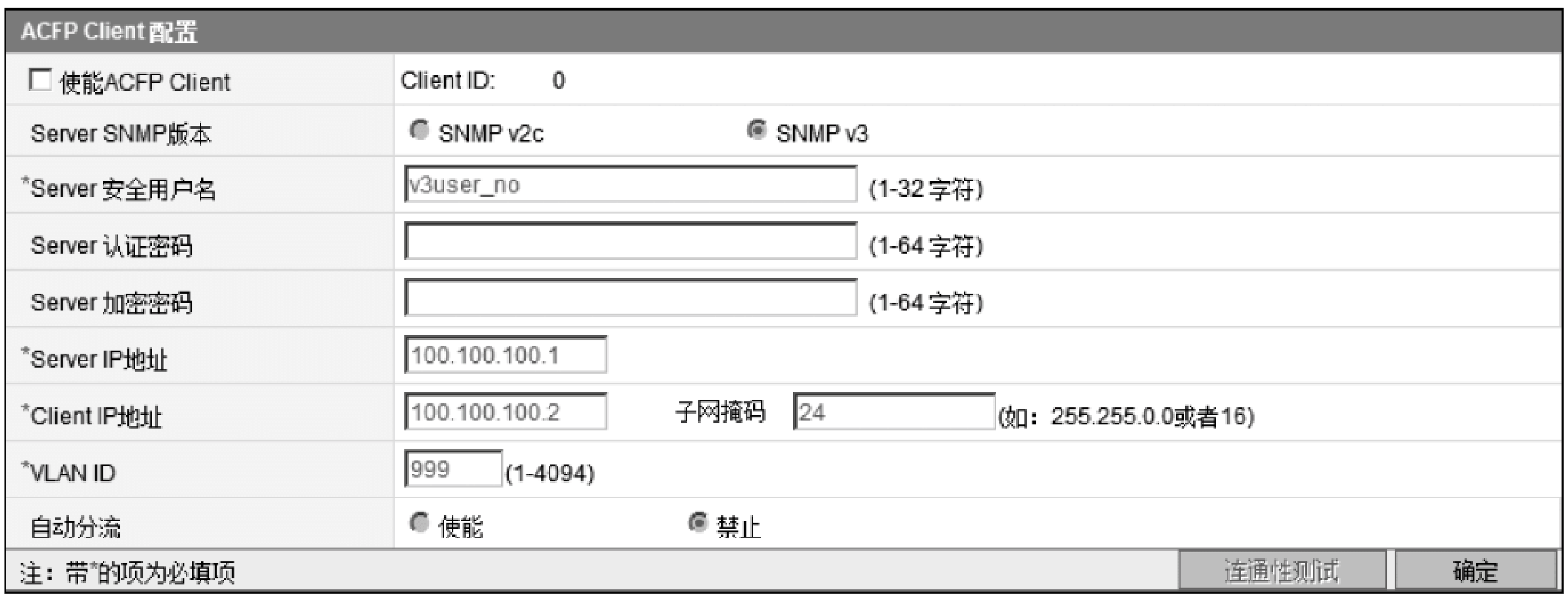


图 6-187　ACFP Client 配置

如果单板未成功注册 acsei，确认内联口未 shutdown 后，请联系 400 处理。

(9) 查看内联口配置

查看交换机内联口配置，是否放通了业务 VLAN 同时下发了防环路 ACL。

命令：*display current-configuration | begin (interface xxx)*

display acl xxx

例如：通过查看内联口配置，确认内联口放通了业务 VLAN，同时配置了过滤策略。

```
<H3C>display current-configuration | begin (interface Ten-GigabitEthernet4/0/1)
#
interface Ten-GigabitEthernet4/0/1
 port link-mode bridge
 description to_ACG
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20
 stp disable
 packet-filter 4000 outbound
 packet-filter 4000 inbound
 mac-address mac-learning disable
```

port trunk permit vlan 10 20 表示放通业务 VLAN；stp disable 表示关闭此接口生成树协议；packet-filter 4000 outbound 表示出方向过滤非业务报文；packet-filter 4000 inbound 入方向过滤非业务报文；mac-address mac-learning disable 关闭 MAC 地址学习功能。

通过查看 ACL，确认过滤规则的配置。

```
<H3C>display acl 4000
Ethernet frame ACL  4000, named -none-, 3 rules,
filter
ACL's step is 5
 rule 0 permit type 0800 ffff dest-mac0cda-41b6-41d8 ffff-ffff-ffff
 rule 50 permit type 88a7 ffff
 rule 100 deny
```

rule 0 permit type 0800 ffff dest-mac 0cda-41b6-41d8 ffff-ffff-ffff 表示放通业务报文；rule 50 permit type 88a7 ffff 表示放通 ACSEI 注册报文；rule 100 deny 表示拒绝非业务报文。

（10）查看 MQC 配置

查看交接口下 MQC 配置，确认配置正确下发，同时与 IPS/ACG 上安全域配置相匹配。

命令：*display qos policy interface xxx*

display acl xxx

例如：通过查看接口下 QOS 配置，确认引流规则正确下发。

```
<H3C>display qos policy interface GigabitEthernet 2/0/2

  Interface: GigabitEthernet2/0/2

  Direction: Inbound

  Policy: up_ACG
   Classifier: up_ACG
        Operator: AND
        Rule(s) : If-match service-vlan-id 10
               If-match destination-mac 0cda-41b6-41d8
               If-match acl 3001
     Behavior: up_ACG
      Redirect enable:
        Redirect type: interface
        Redirect destination: Ten-GigabitEthernet4/0/1
```

Redirect destination：Ten-GigabitEthernet4/0/1 表示重定向的接口。

通过查看 ACL 配置，确认引流地址正确。

```
<H3C>dis acl 3001
Advanced ACL  3001, named -none-, 1 rule,
Match-ALL-Address-Up
ACL's step is 5
 rule 5 permit ip source 10.0.0.0 0.0.0.255
```

rule 5 permit ip source 10.0.0.0 0.0.0.255 表示匹配业务流量。

查看 IPS/ACG 插卡上安全区域配置，确认配置匹配，如图 6-188 所示。

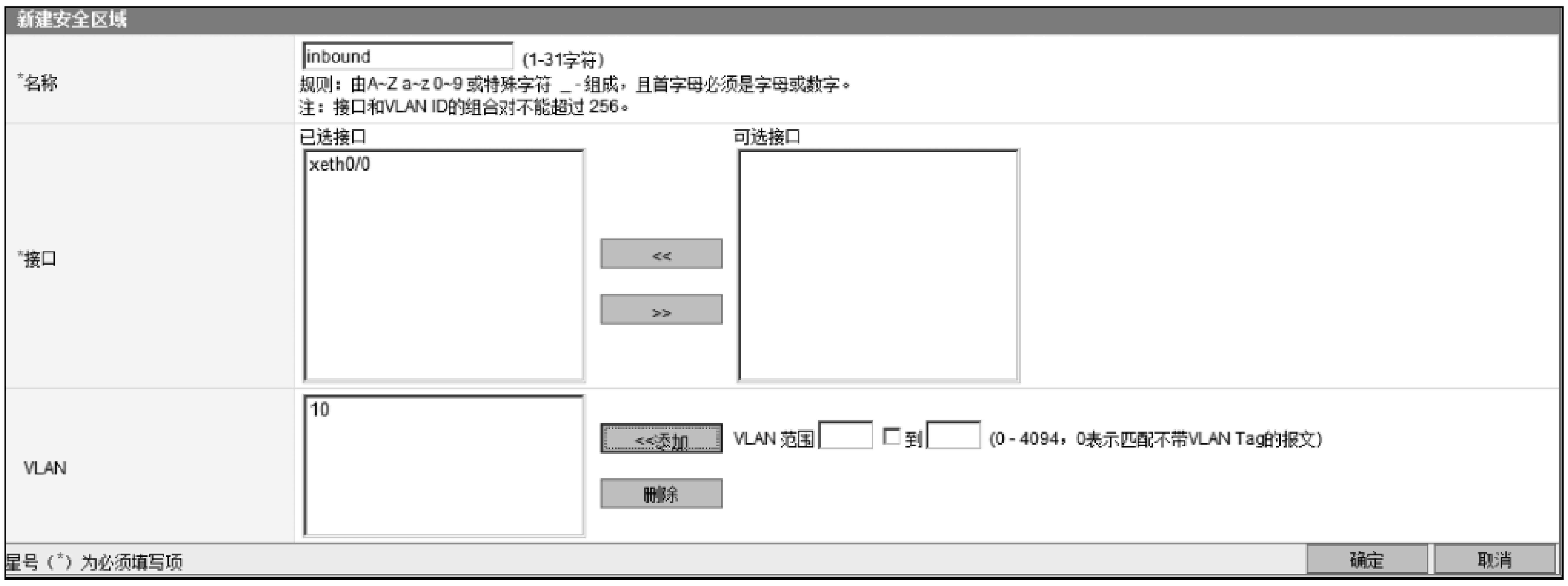


图 6-188 新建安全区域

查看 IPS/ACG 插卡上段配置，确认配置正确，如图 6-189 所示。

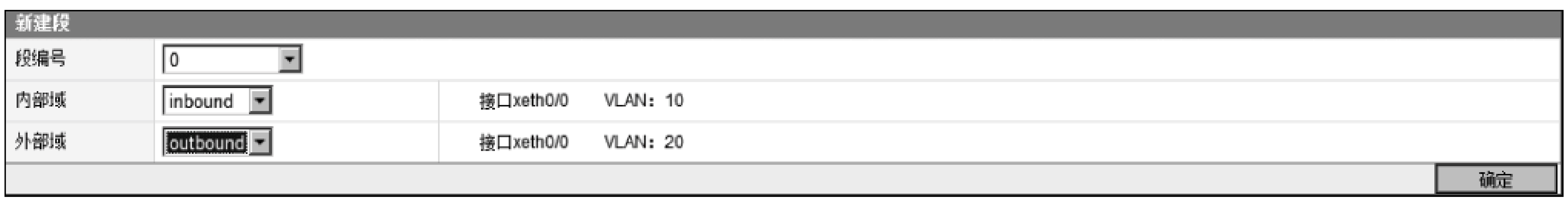


图 6-189 新建段

IPS（ACG）URL过滤功能故障排查

莘启跃



1. 开始

URL(Uniform Resource Locator,统一资源定位符)过滤是一种网页过滤功能。目前 IPS 设备支持自定义 URL 过滤,ACG 设备支持自定义 URL 过滤和分类 URL 过滤。

IPS(ACG)URL 过滤功能定位故障的思路是：首先测试功能是否生效,根据情况来判断是配置问题还是存在设备误识别问题。

2. 流程图相关操作说明

(1) 测试过滤效果

URL 过滤是否生效,可以通过访问被阻断的网站来测试。在未开启"二层回退"的情况下,如果访问的网站被成功阻止,或者被返回应答页面,或者重定向 URL 成功,这说明过滤功能生效,此时如果需要用云图排查,大半是因为日志没有。如果过滤功能有异常,甚至配置无误,那就需要哪找云图的步骤一步步排查了。

(2) 检查日志设置

在成功被 URL 过滤阻断的情况下,无法生成日志需要排查是否开启日志记录或者发送 syslog 功能,syslog 主机是否配置正确。

举例：在导航栏中单击"URL 过滤"→"策略管理",选择"新建自定义规则"选项。如图 6-190 所示,想要看到本地日志,需要选择记录日志时间为"所有时间",这样当有网站访问被审计时会在本地显示日志。

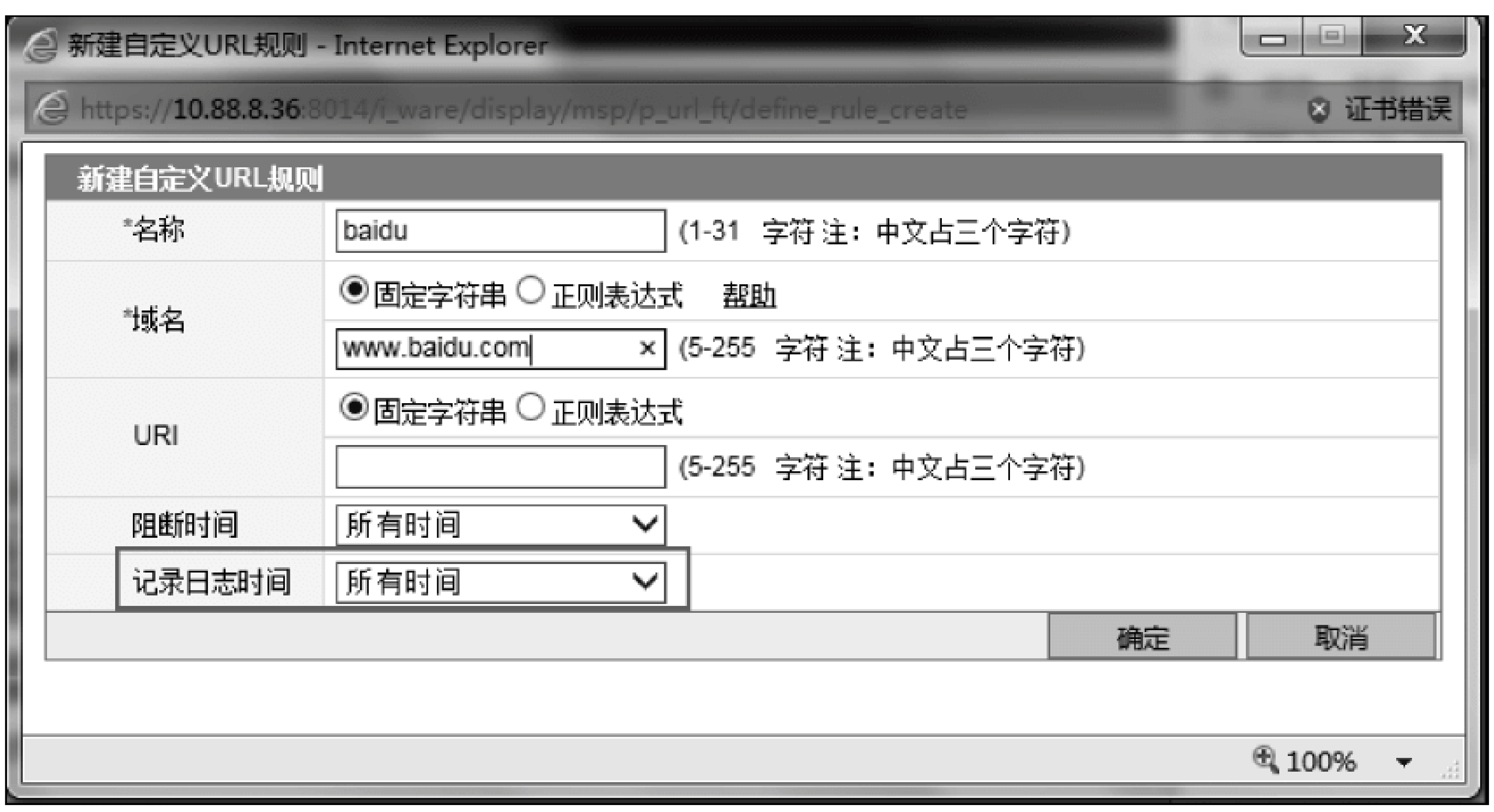


图 6-190　新建自定义 URL 规则

若要将日志输出到 syslog 主机,需要在导航栏中单击"URL 过滤"→"全局配置"选中"输出到 syslog 主机"复选框,并在"日志管理→日志配置→数据日志"中进行主机设置,如图 6-191 和图 6-192 所示。

(3) 检查引流配置

URL 过滤功能要求双向流量都经过设备才能成功生效。如果是单向流,会导致部分或者全部 URL 过滤出现问题。因此,首先要检查双向流量是否引到设备上。



图 6-191　URL 过滤设置

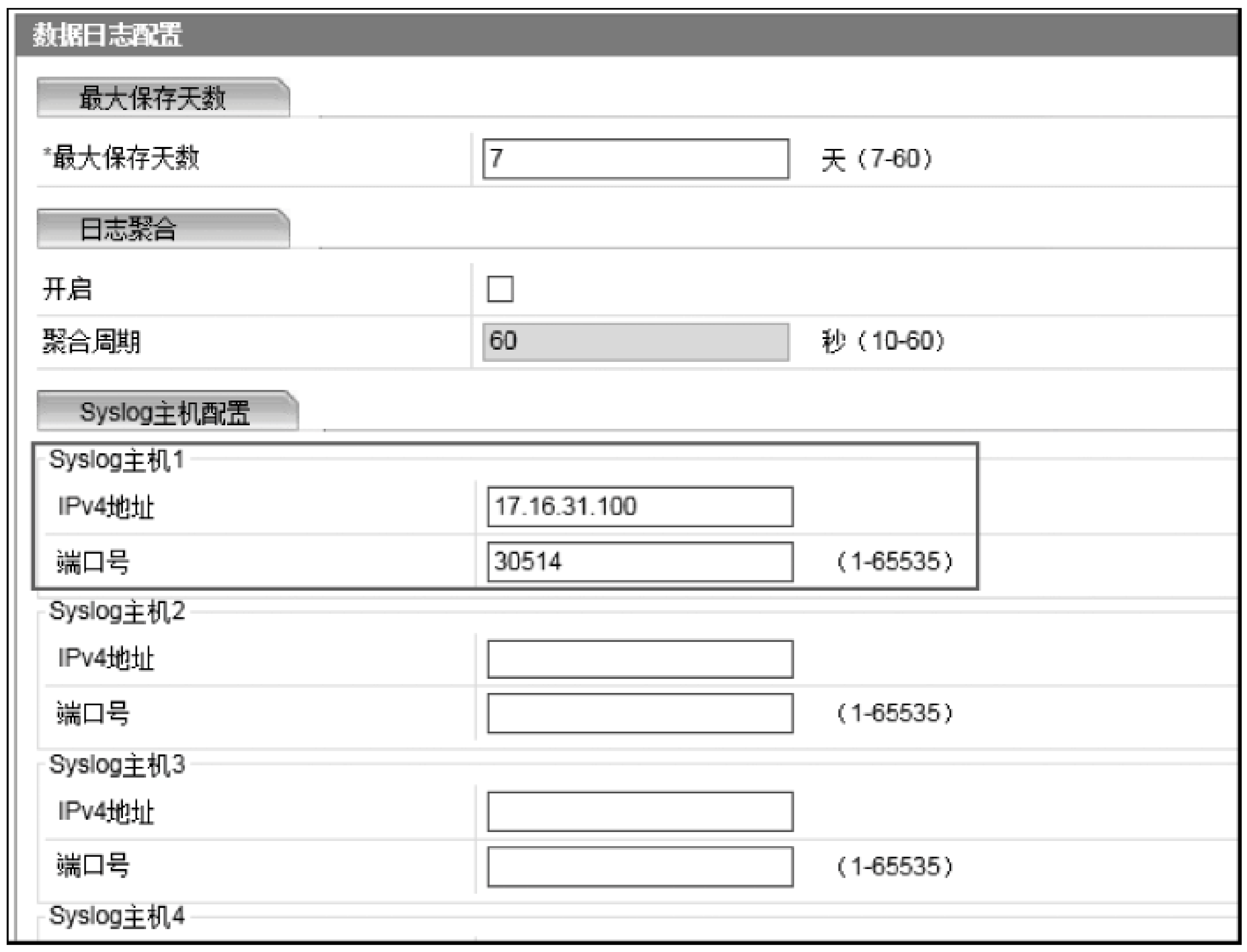


图 6-192　数据日志配置

举例如下。

①“大概看”。在导航栏中单击“报表”→“报文统计”，如图 6-193 和图 6-194 所示，可以看到单向的实时报文统计，如果段的双向都有报文统计，说明双向流量大概都引到了设备上。

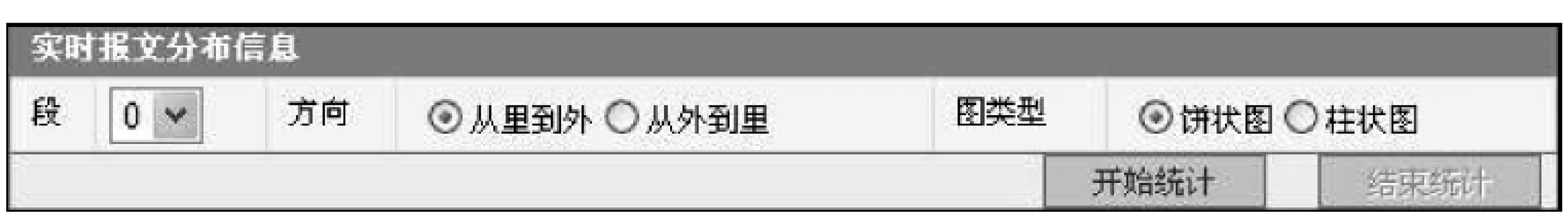


图 6-193　实时报文分布

②“仔细看”。在导航栏中单击“带宽管理”→“策略管理”，新建策略应用，默认规则工作选择“permit＋notify”，通过带宽管理检测所有流量应用。在日志中过滤出想要的五元组日志，如图 6-195 所示，可以看到访问网站的流量是否双向被检测到，如果检测到则说明双向引流成功。

（4）查看功能配置

新建自定义规则的配置是否正确，段下发是否正确；有没有激活策略，匹配的是正则表达式还是固定字符串，都是要注意的地方。

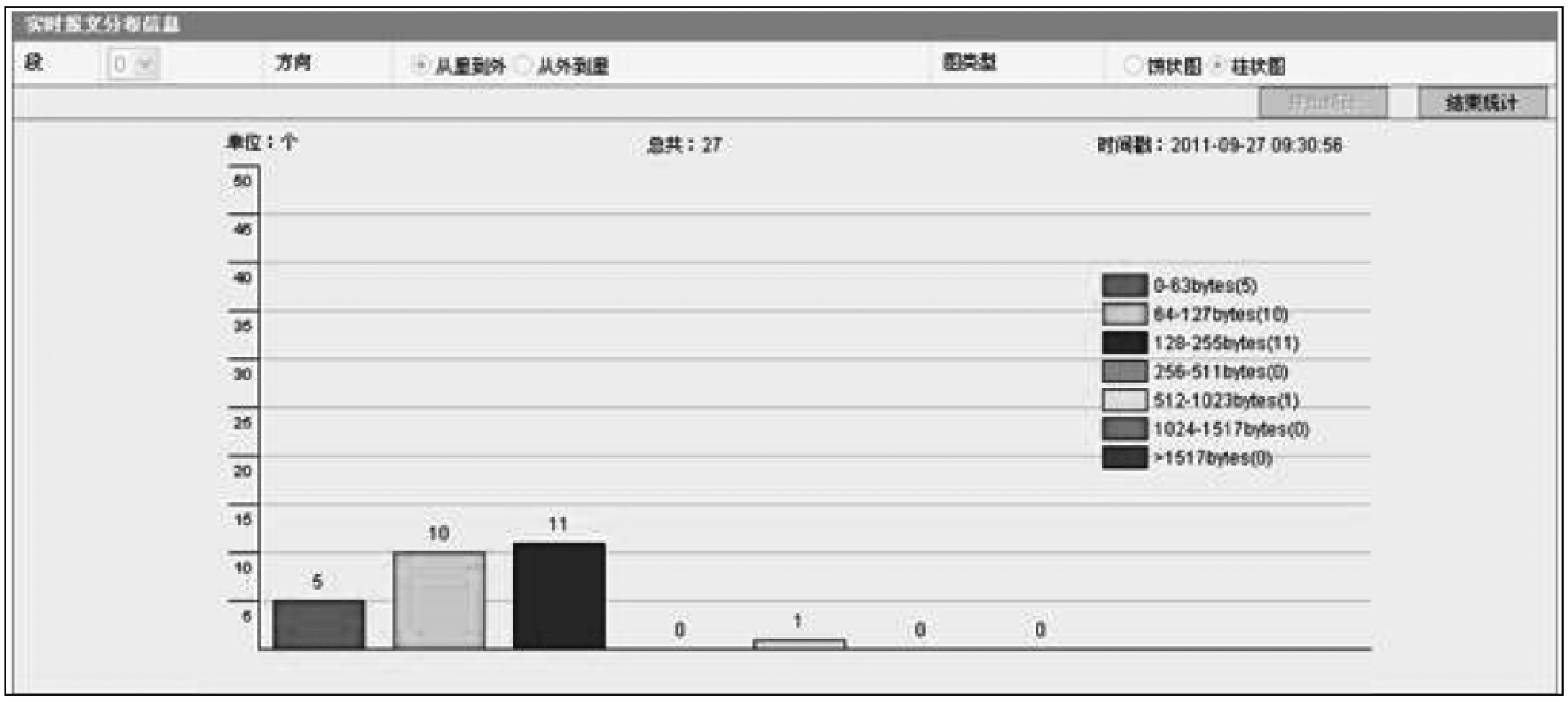


图 6-194 实时报文统计



图 6-195 新建策略应用

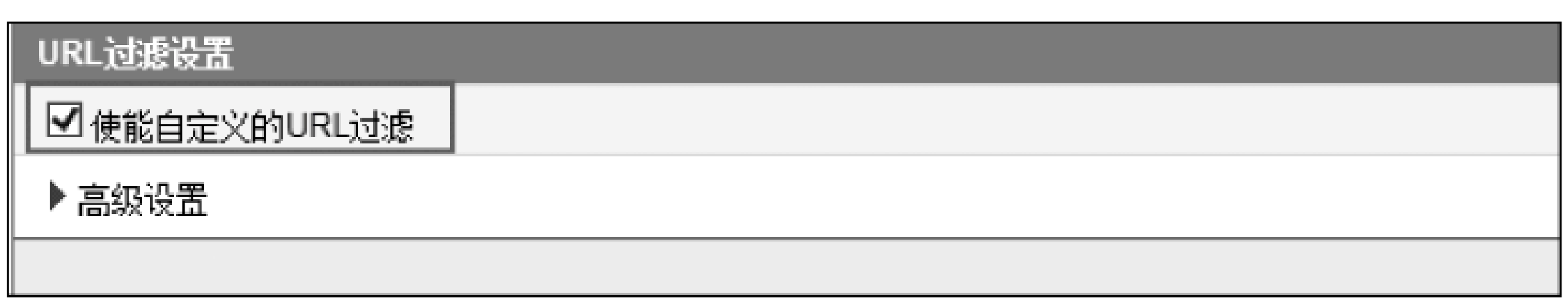


图 6-196 URL 过滤设置

举例：全局下必须选中“使能自定义的 URL 过滤”复选框，如图 6-196 所示。

固定字符串模式下域名全匹配，注意字符串是否正确。如果要匹配含有某个字符串的所有域名，建议使用正则表达式。单击域名正则表达式后面的“帮助”链接，会弹出“正则表达式使用说明”页面，如图 6-197 所示，指导用户如何配置正则表达式，如图 6-197 所示。

阻断时间需要在时间表中管理，具体注意事项可以参考配置手册。

记录日志可以选择不记录或者记录。

配置 URL 过滤时需要注意如下事项。

① 已经应用到段上的 URL 过滤策略不能删除，需要先将策略应用列表中该策略的应用全部删除后，才能删除策略。

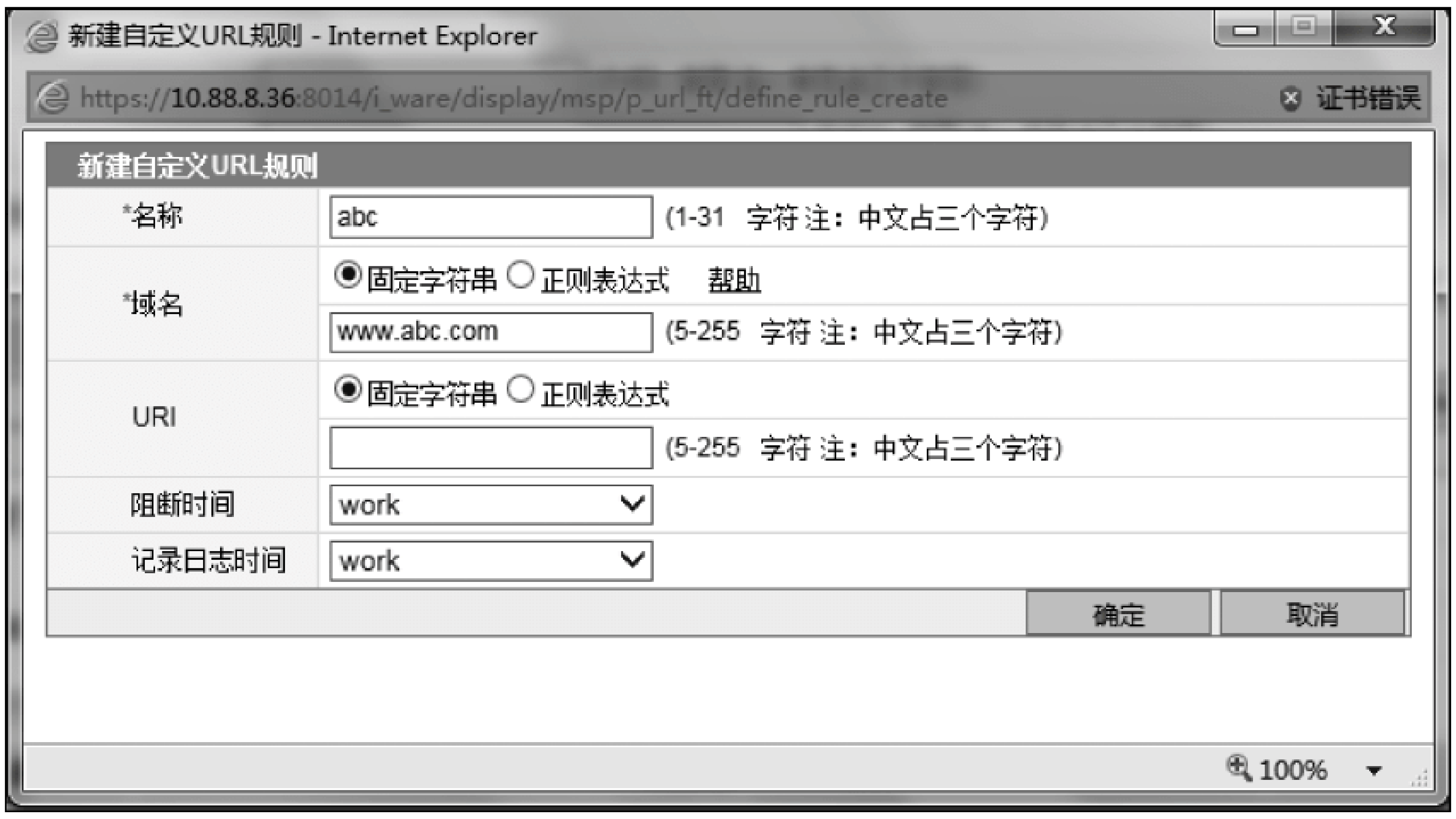


图 6-197　正则表达式使用说明

② 系统预定义的 URL 过滤策略和规则不能删除。

③ 一个报文在一个段上只能匹配一条 URL 过滤策略。当一个段上应用了多个 URL 过滤策略，则系统在对报文进行匹配时，会根据策略应用中指定的 IP 地址组的精确程度，越精确的(即 IP 地址范围越小的)策略应用越优先匹配；当有多个策略应用的 IP 地址范围精确程度相同时，则先配置的策略应用优先匹配。

④ 如果新建策略的过程中某一步骤执行失败，则已经执行过的步骤都将进行回退；而对修改策略的过程，则不会进行回退。

⑤ 分析客户端抓包。有时候会出现的情况即 URL 字符串和域名完全匹配，其他 URL 也成功阻断，就某个网站不生效。URL 自定义检查的是 http 头的 host 字段，因此可以通过客户端抓包找到访问网站的报文，在报文中找到 host 字段，这个字段的 URL 才是真正的 URL。实际域名和 URL 不相符的情况时有发生，请注意。

举例：有用户想限制 taobao 网站，但是在检查了引流，配置之后并未发现问题，换作其他域名可以成功阻断。通过抓包发现，taobao 的 host 字段的内容和过滤规则中 taobao. com 不匹配，可以把图 6-198 中 host 中的字段，log. mmstat. com 作为过滤的关键字，进行过滤。

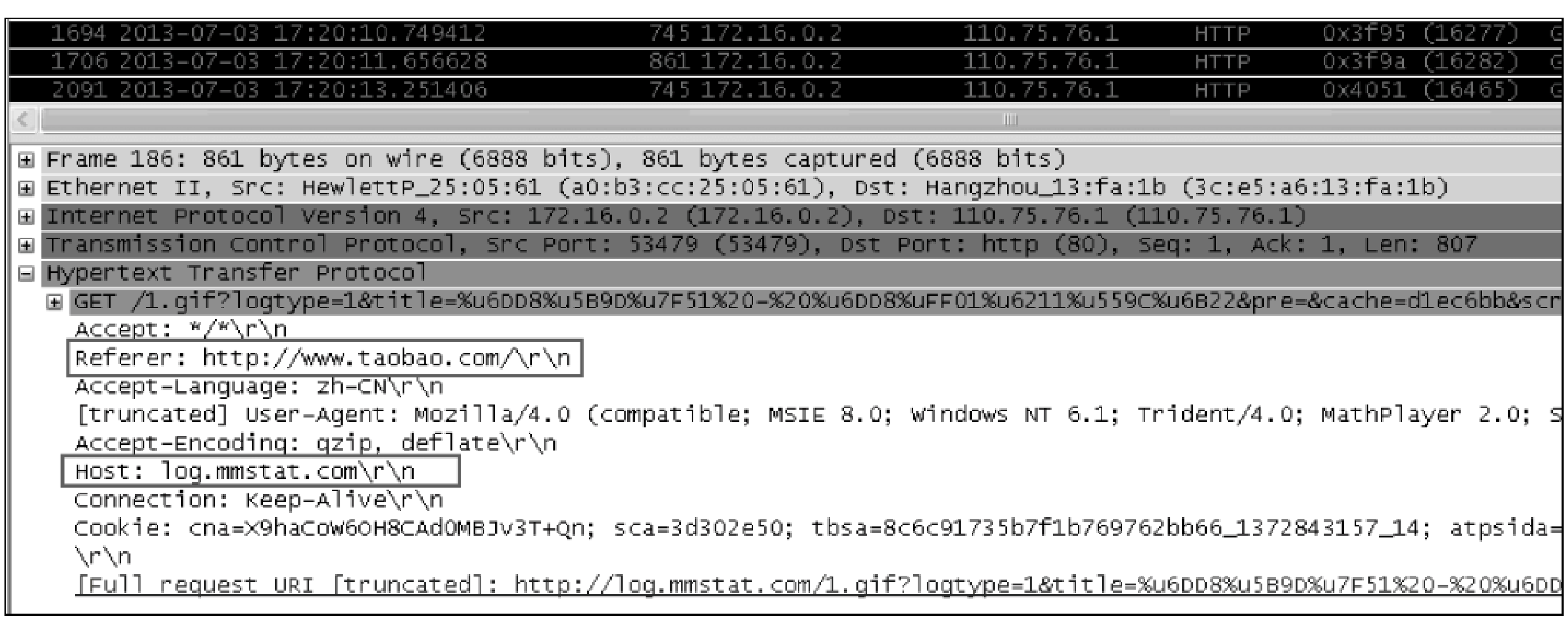


图 6-198　抓包(1)

大多数网站，referer 字段和 host 字段相同，如图 6-199 抓包所示。

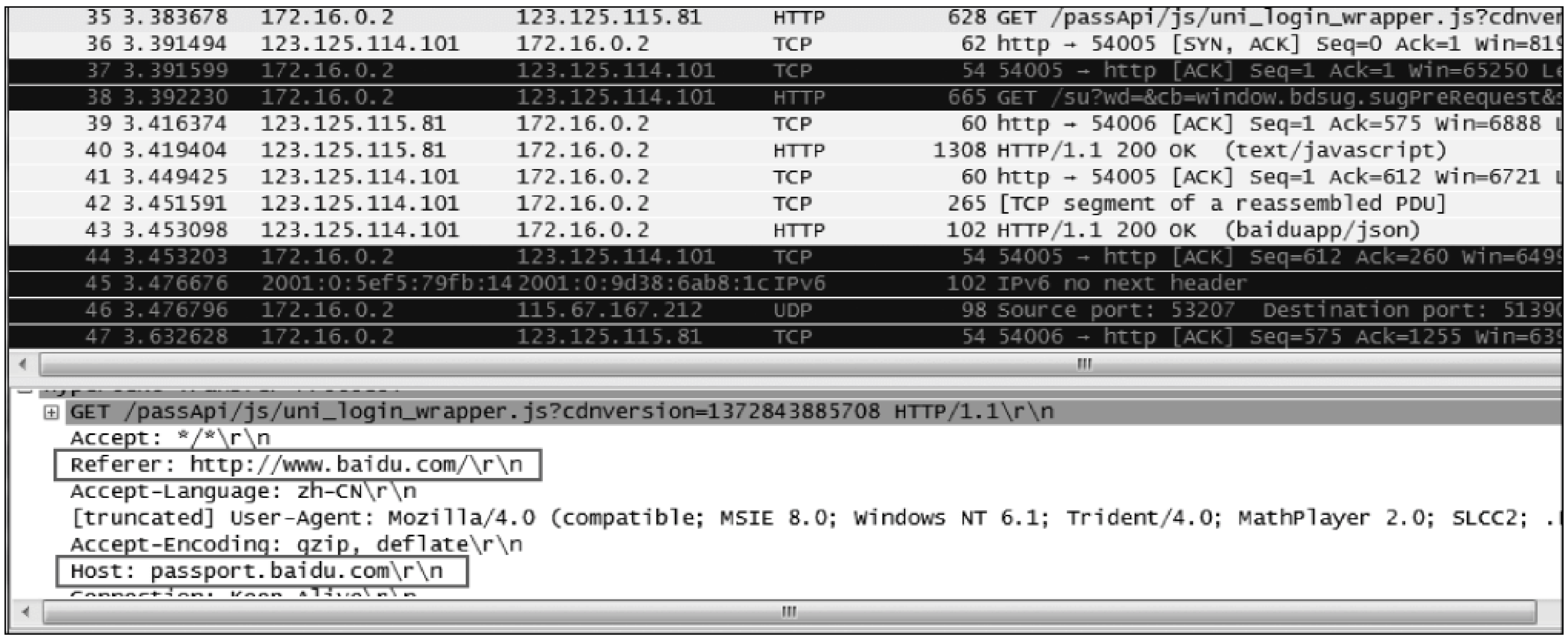


图 6-199 抓包(2)

⑥ 检查是否被误识别。误识别最大的可能就是 Client 或 Server 端对应的 IP 被加入了“P2P 端口对”，被识别成加密 P2P 流量了。这种情况一般会出现用户网络中只是部分用户出现问题的现象。可用下面的方法确认。

举例：配置针对单个测试 IP 的带宽管理策略，default 服务，permit+notify。然后查看服务日志，看看协议是否被识别成 P2P 或其他协议了。如果识别成 P2P 了，登录串口，系统视图下查看是否存在 P2P 节点。

```
[H3C]display p2p
P2P length serial identification is enabled.
P2P precise identification is enabled.
IPv4 UDP negotiate nodes: 0
IPv6 UDP negotiate nodes: 0
IPv4 TCP negotiate nodes: 4
IPv6 TCP negotiate nodes: 0
```

如果有，进入 shell 视图(如何进入 shell 视图请咨询总部工程师)，检查 P2P 端口对信息。

假设测试 IP 地址为 a.b.c.d，计算 c*256+d=e，然后执行以下命令。

命令：*uaae_test -s T e*

uaae_test -s U e

dmesg -c

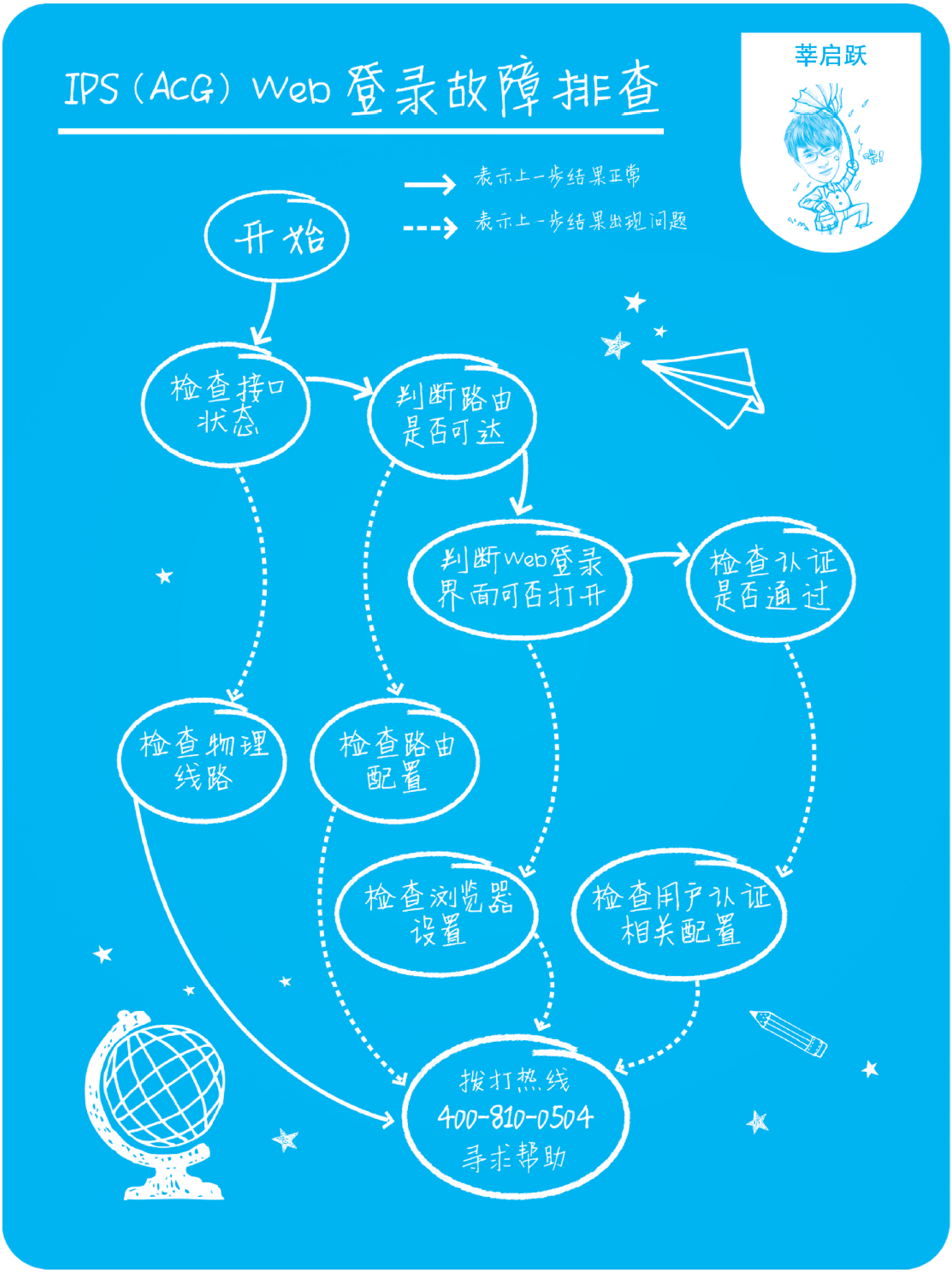
dmesg 显示的信息中如果出现了 a.b.c.d，说明该 IP 被加入端口对了，将其清除即可。

清除端口对的命令。

命令：*uaae_test -s C*

说明：加入端口对的 IP 地址，应该是之前有过加密 P2P 下载的动作，遇到端口对的存在影响了其他应用的情况，不能简单归结为设备加密 P2P 识别有问题。具体问题具体分析。

误识别问题请收集信息反馈总部工程师作进一步分析。


IPS（ACG）Web登录故障排查
莘启跃
表示上一步结果正常
表示上一步结果出现问题
开始
检查接口状态
判断路由是否可达
判断Web登录界面可否打开
检查认证是否通过
检查物理线路
检查路由配置
检查浏览器设置
检查用户认证相关配置
拨打热线
400-810-0504
寻求帮助

1. 开始

IPS/ACG 为应用层安全产品，提供 4～7 层安全，用户可以通过 Web 客户端登录设备进行配置管理与维护。

IPS/ACG Web 登录故障的定位思路是：首先检查物理线路，之后排查浏览器设置，最后检查用户认证相关配置。

2. 流程图相关操作说明

(1) 检查接口状态

分别查看两端设备的接口、协议状态是否 Up。如果接口状态为 Down，则说明物理层配置、线缆问题。

命令：*display interface* [*interface name*]

例如：通过命令查看 IPS/ACG meth0/2 当前状态 Up，协议 Up，如果接口当前状态为 Down 或者协议为 Down，则判断该接口状态异常。

```
<H3C>display interface meth0/2
Interface meth0/2
    input packets 1323213677, bytes 1639640697
    output packets 226530, bytes 25619797
    administration state Up, line state Up
    1000Mbps-speed mode, full-duplex mode
    Link speed type is autonegotiation, link duplex type is autonegotiation
    combo enable copper
    inet add: 10.153.42.87, Mask 255.255.255.0
```

(2) 检查物理线路

根据不同接口类型选配相应的接口线缆，并确保线缆连接正确；通过命令可以查看接口的双工、速率、协商类型、光/电口类型。

命令：*display interface* [*interface name*]

例如：通过命令查看 IPS/ACG meth0/2 的双工、速率、协商类型、光/电口类型。

① speed mode：当前速率模式。

② duplex mode：当前双工模式。

③ Link speed type：速率配置类型，autonegotiation 表示自协商，force link 表示用户配置。

④ link duplex type：双工配置类型，autonegotiation 表示自协商，force link 表示用户配置。

⑤ combo enable：combo 接口的激活状态，copper 表示电口被激活，fiber 表示光口被激活。

```
<H3C>display interface meth0/2
Interface meth0/2
    input packets 1323213677, bytes 1639640697
```

```
output packets 226530, bytes 25619797
administration state Up, line state Up
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
combo enable copper
inet add: 10.153.42.87, Mask 255.255.255.0
```

当 IPS/ACG 的接口速率、双工模式、光/电口类型与客户端均一致时才正常。

(3) 判断路由是否可达

命令：*ping x.x.x.x*

例如：通过命令查看，可以确认 IPS/ACG 与客户端之间路由可达。

```
<H3C>ping 10.10.241.239
PING 10.10.241.239 (10.10.241.239) 56(84) bytes of data.
64 bytes from 10.10.241.239: icmp_seq=1 ttl=126 time=3.00 ms
64 bytes from 10.10.241.239: icmp_seq=2 ttl=126 time=72.0 ms
64 bytes from 10.10.241.239: icmp_seq=3 ttl=126 time=4.00 ms
64 bytes from 10.10.241.239: icmp_seq=4 ttl=126 time=3.00 ms

--- 10.10.241.239 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 3.000/20.500/72.000/29.736 ms
```

(4) 检查路由配置

如客户端与 IPS/ACG 管理口直连，确保二者在同一网段即可，不需再检查路由。

① 查看 IPS/ACG 的路由表中是否存在到达客户端的路由。

命令：*display ip route-static*

例如：通过命令查看，可以确认 IPS/ACG 上有到达客户端的路由 0.0.0.0 0.0.0.0，下一跳是 10.153.42.1。

```
[H3C]display ip route-static
Destination          Genmask            Gateway
10.153.42.0          255.255.255.0      0.0.0.0
0.0.0.0              0.0.0.0            10.153.42.1
```

② 查看客户端是否有到 IPS/ACG 的路由。

命令：*route print*

例如：通过命令查看，客户端有到 IPS/ACG 的路由 0.0.0.0 0.0.0.0，下一跳是 10.10.240.1，此时需检查 10.10.240.1 上是否有到达 IPS/ACG 的路由。

```
C:\Users\H3C>route print
IPv4 路由表
==========================================================================
活动路由:
网络目标         网络掩码          网关          接口        跃点数
          0.0.0.0          0.0.0.0     10.10.240.1   10.10.241.239     25
      10.10.240.0    255.255.248.0          在链路上    10.10.241.239    281
```

当 IPS/ACG 和客户端之间均有到达对方的路由，则判断路由无问题。

（5）判断 Web 登录界面可否打开

IPS/ACG 默认开启 HTTPS 登录方式且不可关闭，通过浏览器访问 https://x. x. x. x 检查 Web 登录界面是否能打开，如图 6-200 所示。



图 6-200 登录界面(1)

图 6-201 为正常打开的 IPS/ACG Web 登录界面。



图 6-201 登录界面(2)

（6）检查浏览器设置

建议使用 IE 浏览器，对于高版本浏览器，可设置兼容性视图，并加入可信站点。

兼容性视图设置路径：“浏览器工具→兼容性视图设置→添加”。兼容性视图设置如图 6-202 所示。

加入可信站点路径：“浏览器工具→ Internet 选项→安全→受信任的站点→站点→添加”。受信任站点如图 6-203 所示。

说明：如浏览器设置正常但还是不能打开 Web 登录界面，则需收集设备的诊断信息、版本信息、系统日志、操作日志及浏览器截图。

命令：*collect diag_info* [*TFTP SERVER IP*]

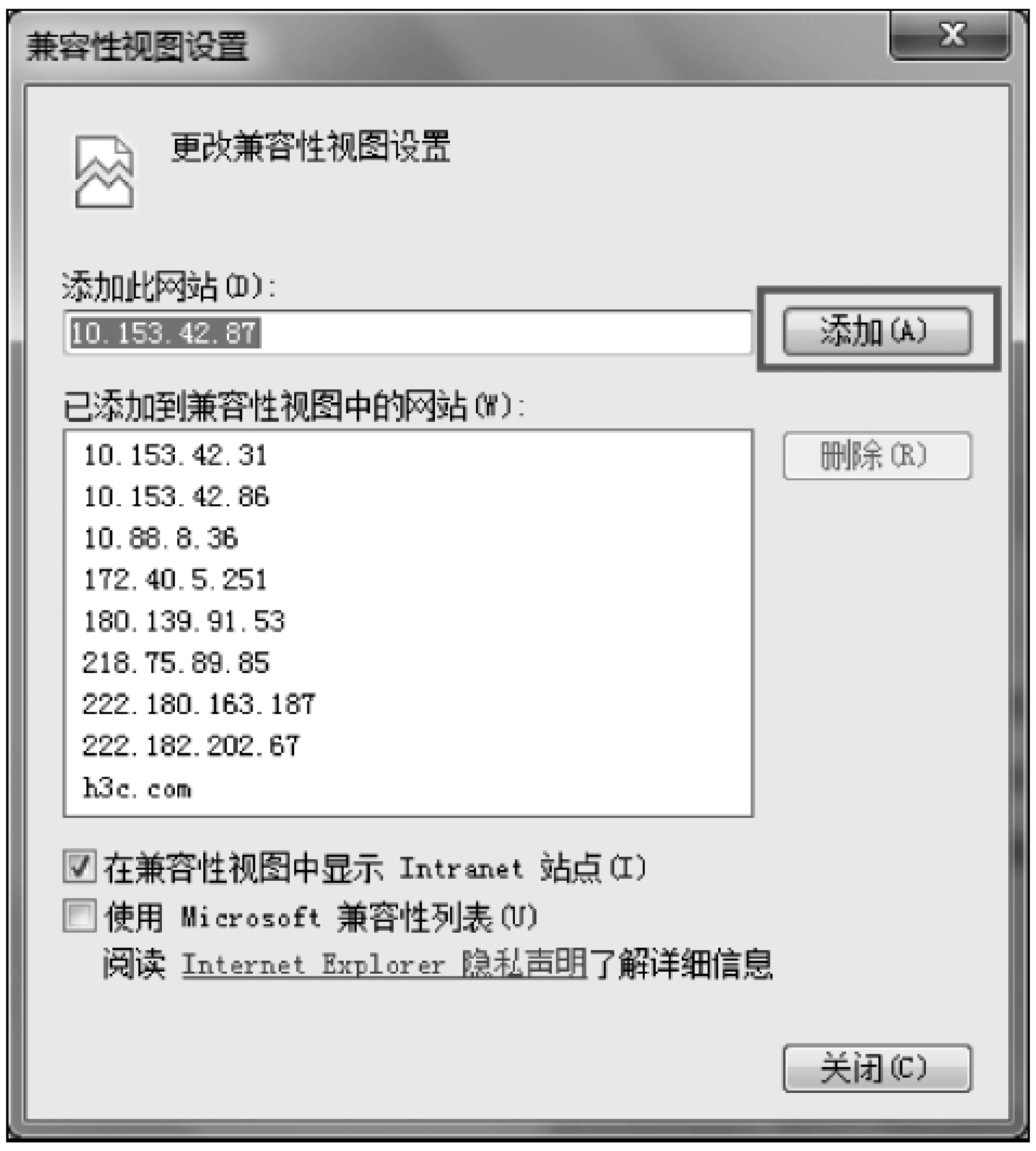


图 6-202　兼容性视图设置



图 6-203　受信任站点

例如：通过命令将 IPS/ACG 的诊断信息导出至 TFTP 服务器 10.10.241.239，如图 6-204 所示。

```
[H3C]collect diag_info 10.10.241.239
```

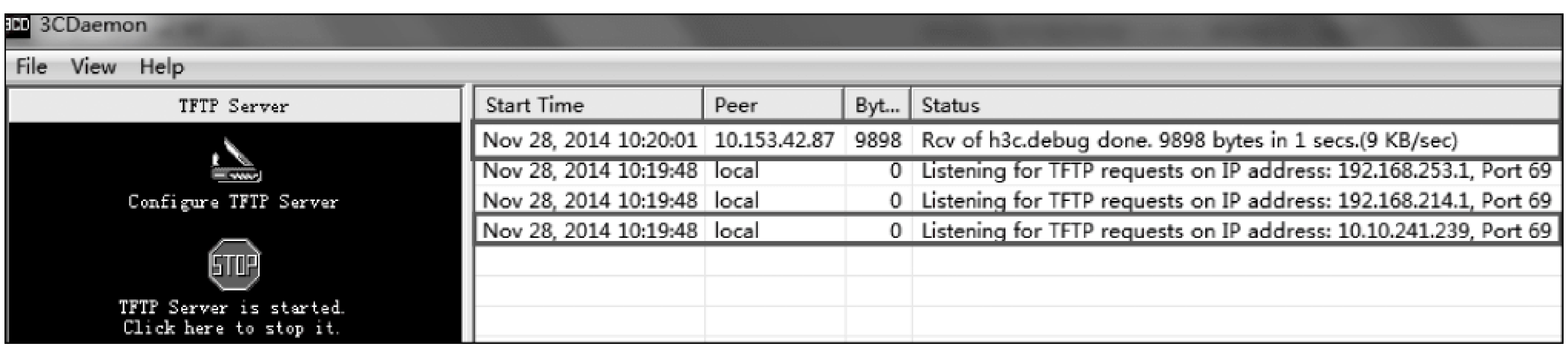


图 6-204　3CDaemon

命令：*display version*

例如：通过命令查看 ACG 的版本信息。

```
<H3C>display version
 H3C i-Ware Platform Software
i-Ware software, Version 1.10, Ess 6119P06
 Signature database, Version APP 1.1.265
Copyright (c) 2004-2014 Hangzhou H3C Technologies Co., Ltd. All rights reserved.
 Without the owner's prior written consent, no decompiling nor reverse-engineering shall be allowed.
SecBlade ACG Uptime is 0 week(s), 2 day(s), 00 hour(s), 28 minute(s)

 CPU type:   RMI XLR732
 Flash Memory: 4M bytes
 CF card Memory: 249M bytes

 Pcb                 Version:  Ver.A
 CPLD                Version:  1.0
```

```
BASIC BOOTWARE           Version:  1.19
 EXTEND BOOTWARE         Version:  1.19
 [SLOT  0]  LSQ1ACGASC0 (hardware)Ver.A,  (Driver)1.0,   (Cpld)  1.0
```

系统日志收集路径:“日志管理→系统日志→日志查询→查询→导出到 CSV”。

操作日志收集路径:“日志管理→操作日志→日志查询→查询→导出到 CSV”。

(7) 判断认证是否通过

在 Web 登录界面输入用户名/密码后,如登录成功,设备会跳转至主界面,否则页面会弹出提示信息。

设备主界面如图 6-205 所示。

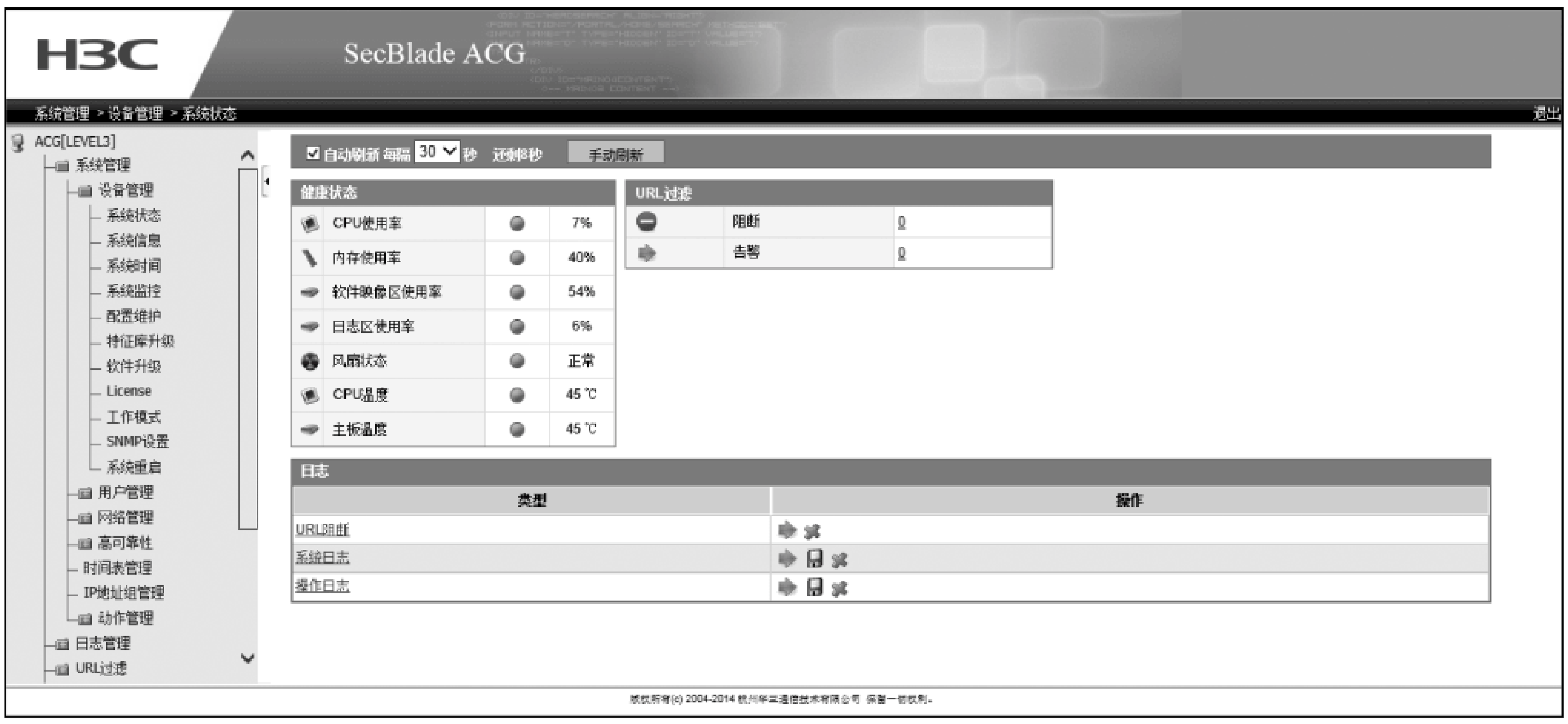


图 6-205 设备主界面

登录不成功时页面可能出现如图 6-206～图 6-208 所示提示信息。



图 6-206 提示信息(1)



图 6-207 提示信息(2)



图 6-208 提示信息(3)

(8) 检查用户认证相关配置

① IPS/ACG 登录采用本地认证方式。IPS/ACG 默认管理员账号/密码为 admin/admin,该账号不可删除,管理员可修改此密码。

当登录界面提示用户名/密码错误或者提示用户已经被锁定时,首先确认用户名/密码是否正确。对于普通用户,如忘记用户名/密码或是账号被锁定,可联系管理员处理,管理员可修改普通用户的密码及解除账号锁定。对于管理员,如忘记 Web 登录密码,则只能进入命令行重置密码。

命令:*reset web-admin-user-password*

例如：通过命令重置管理员账号 admin 的 Web 登录密码，如图 6-209 所示。

```
[H3C] reset web-admin-user-password
```



图 6-209　修改密码

说明：默认情况下，当连续 3 次输入密码错误，则对应的用户名被锁定 30 分钟，可等待 30 分钟重新输入用户名/密码，或者具有 LEVEL 3 级别的用户手工解除锁定。管理员可在安全策略中进行参数配置，如图 6-210 所示。

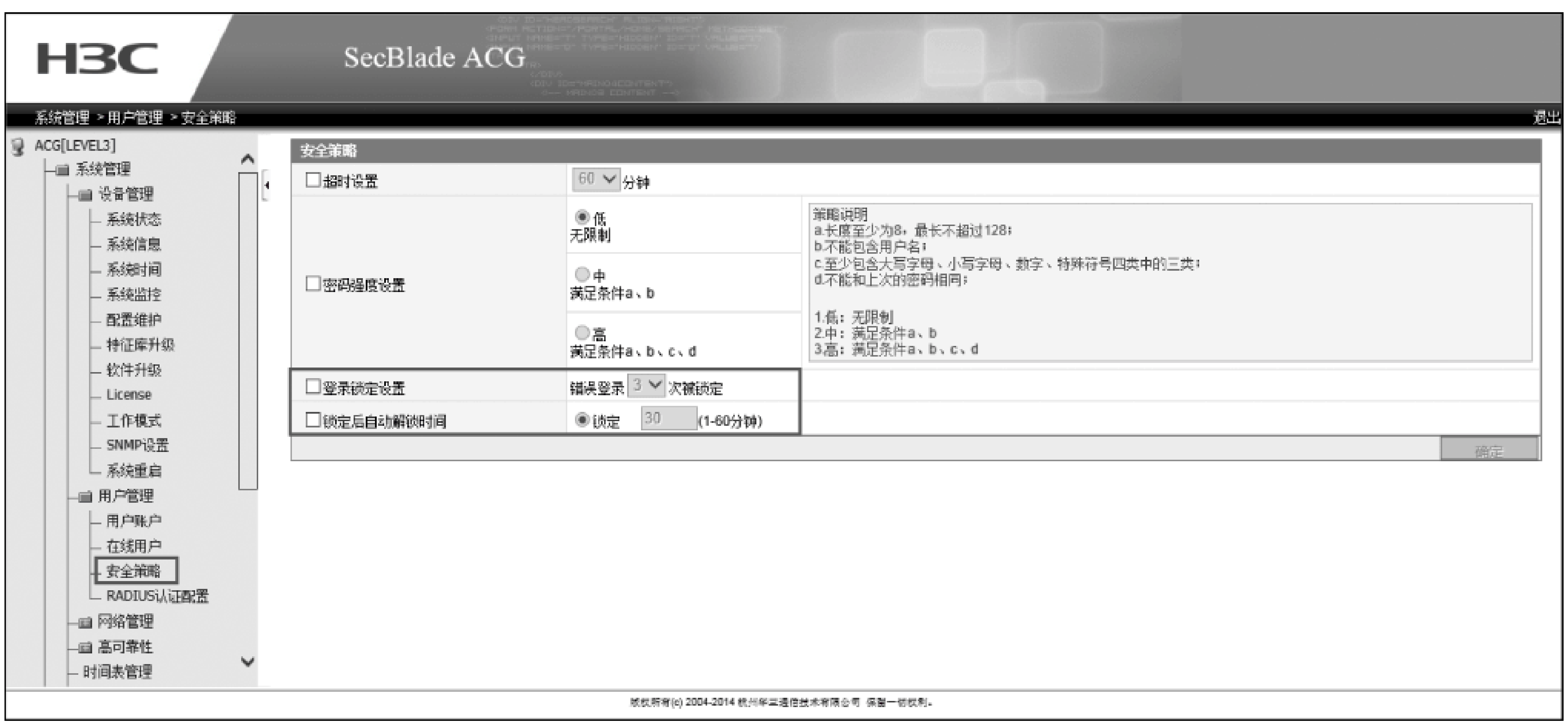


图 6-210　配置锁定用户名时间

② IPS/ACG 登录采用 RADIUS 认证。由于 RADIUS 协议采用 UDP 报文来承载数据，因此通信过程是不可靠的。如果在指定的服务器应答超时时间内没有收到服务器的响应，则设备有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果发送 RADIUS 请求报文的累计次数超过指定的最大尝试发送次数而 RADIUS 服务器仍旧没有响应，则设备将尝试与其他服务器通信，如图 6-211 所示。

说明：使能 RADIUS 认证功能后，用户通过 Web 登录设备均采用 RADIUS 认证，本地认证不再生效，即不能再通过本地用户名/密码 Web 登录设备。如需恢复至本地认证，则应在命

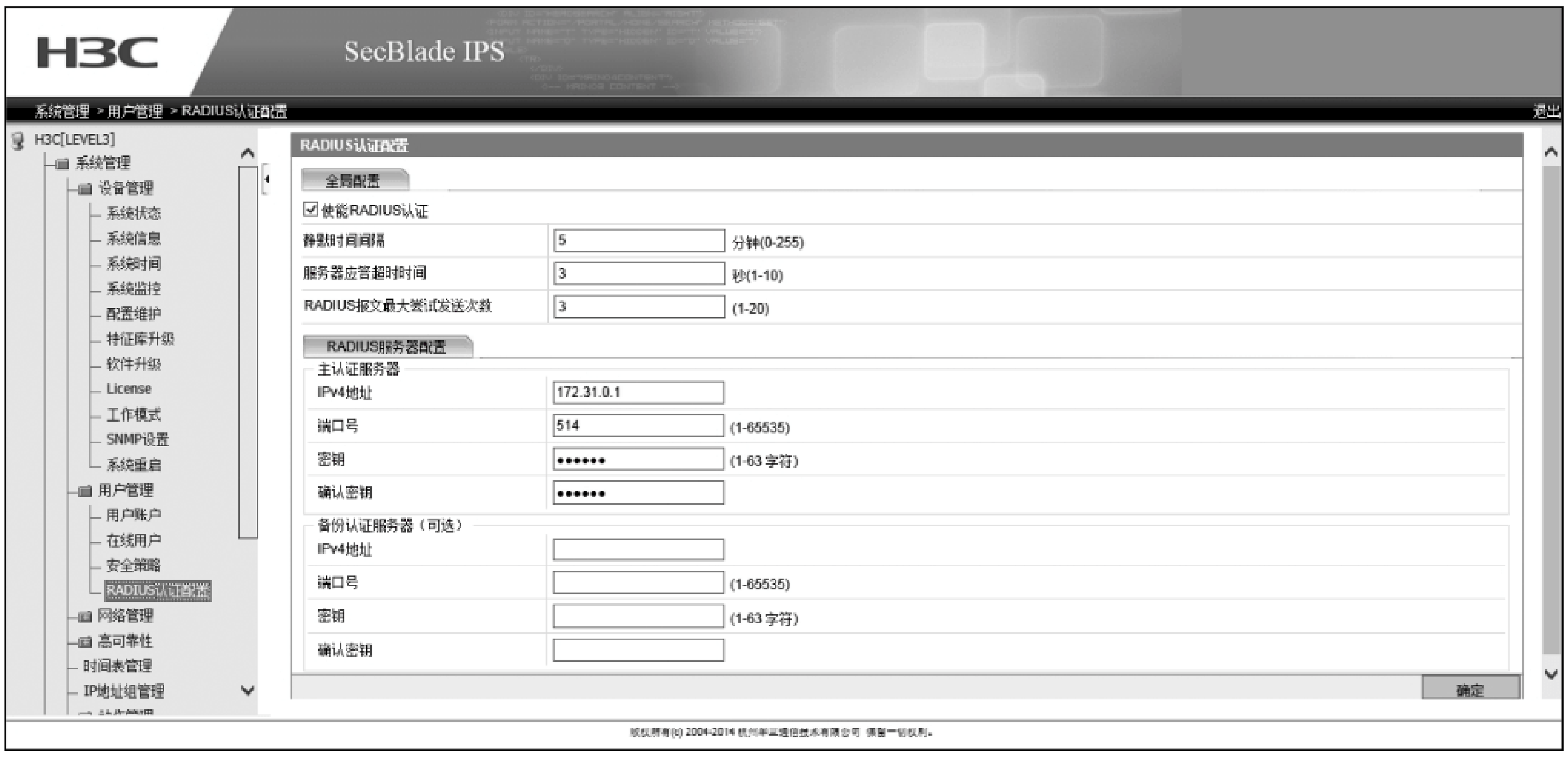


图 6-211　RADIUS 认证配置

令行系统视图下执行相关命令。

命令：*disable web-radius-auth*

例如：通过命令恢复至本地认证。

```
[H3C] disable web-radius-auth
```

IPS（ACG）带宽管理功能故障排查

刘林涛





1. 开始

网络流量按照其用途的不同划分成不同的服务类型，例如 E-mail 服务、VoIP 服务等，对不同的服务类型实施不同的管理控制行为，称为带宽管理。因此，带宽管理包括两个主要部分：服务和针对一个具体服务的控制行为。

IPS/ACG 带宽管理定位故障的思路是，通过查看设备工作模式，引流配置，确认设备二层回退状态，查看带宽管理全局配置，查看带宽管理具体配置等步骤逐步排查，确认问题所在。

2. 流程图相关操作说明

(1) 查看设备工作模式

通过登录 ACG 插卡，查看设备目前的工作模式：直连或者旁路。如果为旁路部署，需修改为直连部署。

例如：通过 Web 页面查看 ACG 当前工作模式，如图 6-212 所示。



图 6-212 工作模式

通过 Web 页面，可以查看到连接模式处于直连模式，应用模式为完整功能集，在此情况下，带宽管理的限速策略才能生效。

(2) 查看设备引流配置

通过登录 ACG 插卡，查看设备安全域配置，确认设备内部域接口和外部域接口选择无错误。

例如：如图 6-213 所示，通过 Web 页面查看，内部域所选端口为连接内网端口，外部域所选端口为连接外部域端口，如图 6-214 所示。

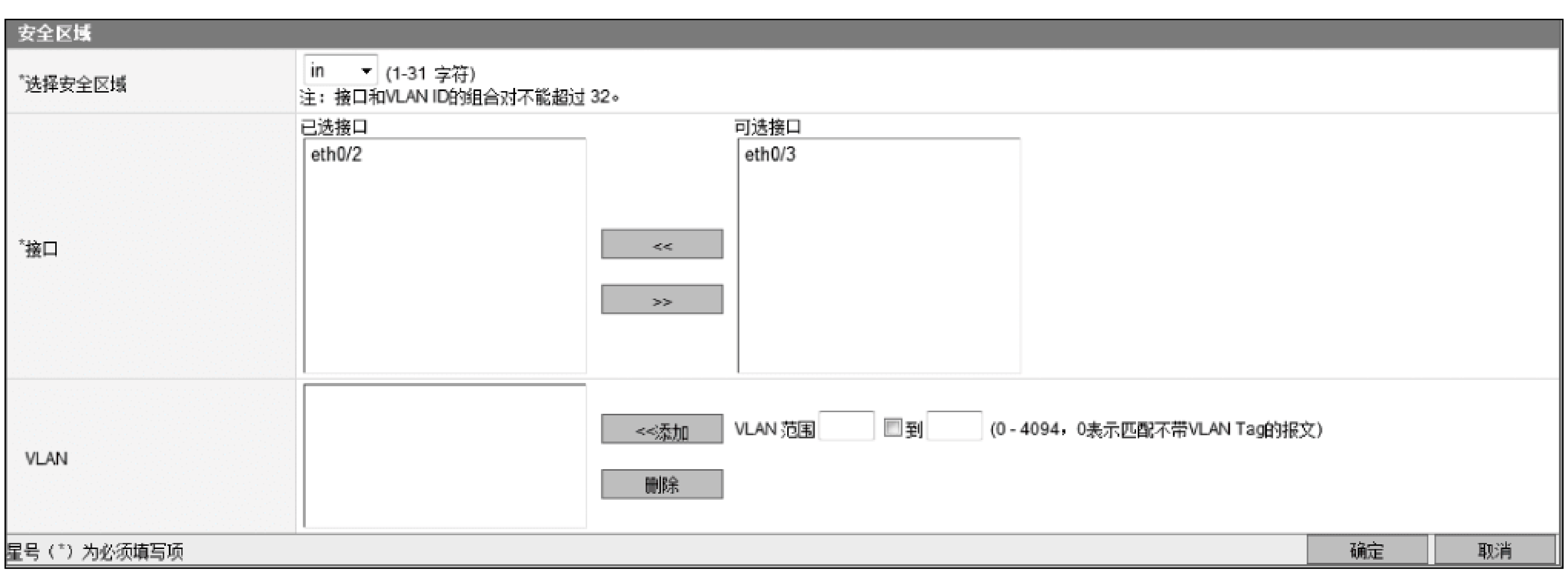


图 6-213 安全区域(1)

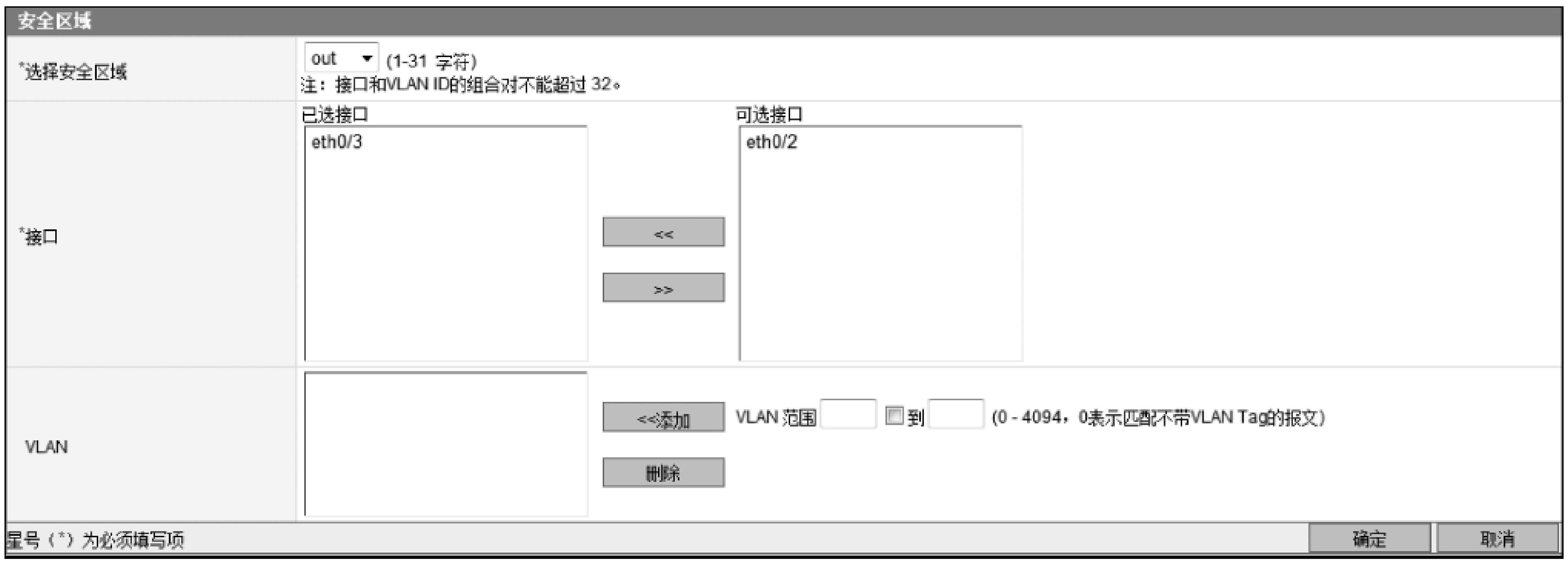


图 6-214　安全区域(2)

由图 6-213、图 6-214 可以看出内部域端口定义为 eth0/2，外部域端口定义为 eth0/3。

查看 ACG 上段配置，确认内部域以及外部域成功关联，并正确调用。

例如：通过 ACG 插卡的 Web 页面，查看 ACG 插卡段配置，如图 6-215 所示。

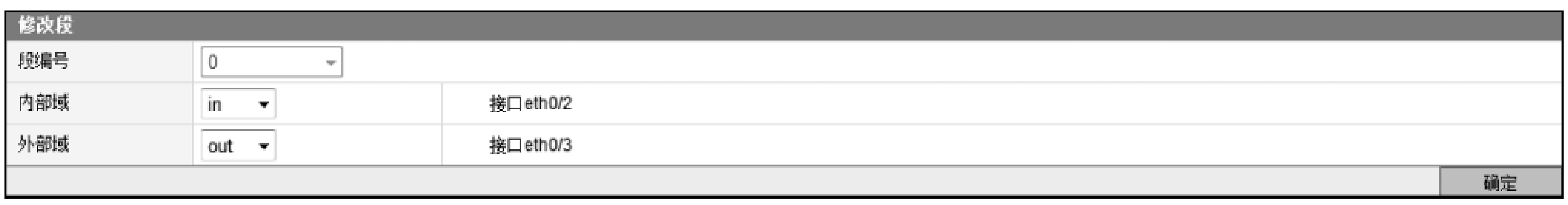


图 6-215　修改段

如图 6-215 所示，通过查看段配置，确认内部域为 in，接口为 eth0/2，外部域为 out，接口为 eth0/3，关联段为 0。

(3) 查看二层回退状态

查看 ACG 插卡二层回退状态，确认设备处在正常工作状态。

例如：通过 Web 页面，查看设备二层回退状态，设备是否使能了二层回退，如图 6-216 所示。

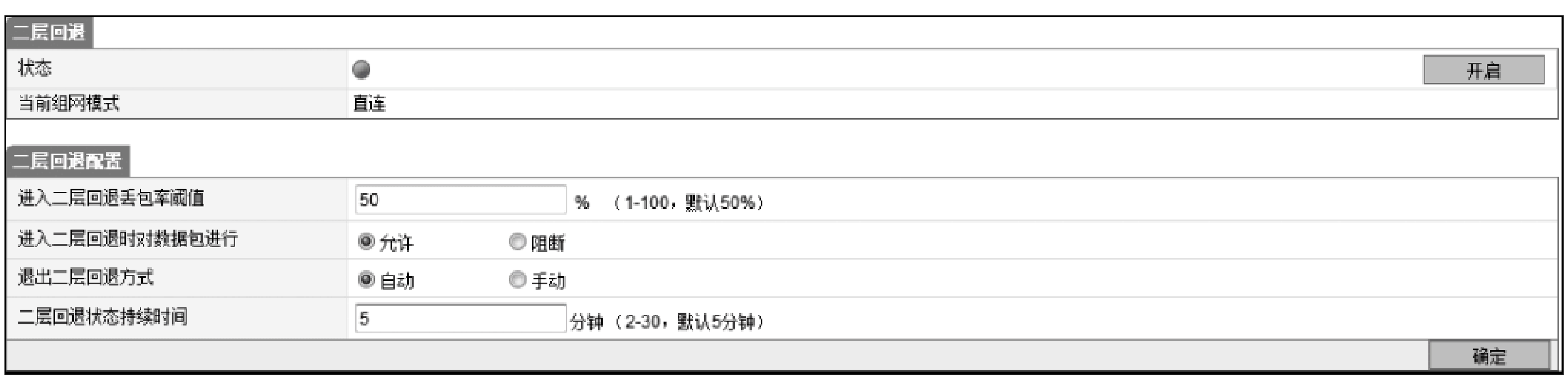


图 6-216　二层回退状态

如图 6-216 所示，通过查看设备二层回退状态，确认设备未使能二层回退功能，当前设备处于正常工作模式。

(4) 查看引流功能

带宽管理功能要求双向流量都经过设备才能成功生效。如果是单向流，会导致部分或者全部带宽管理出现问题。因此，首先要检查双向流量是否引到设备上。

例如如下几方面。

①“大概看”。在导航栏中单击“报表”→“报文统计”,可以看到单向的实时报文统计,如果段的双向都有报文统计,说明双向流量大概都引到了设备上,如图 6-217 和图 6-218 所示。



图 6-217 实时报文分布

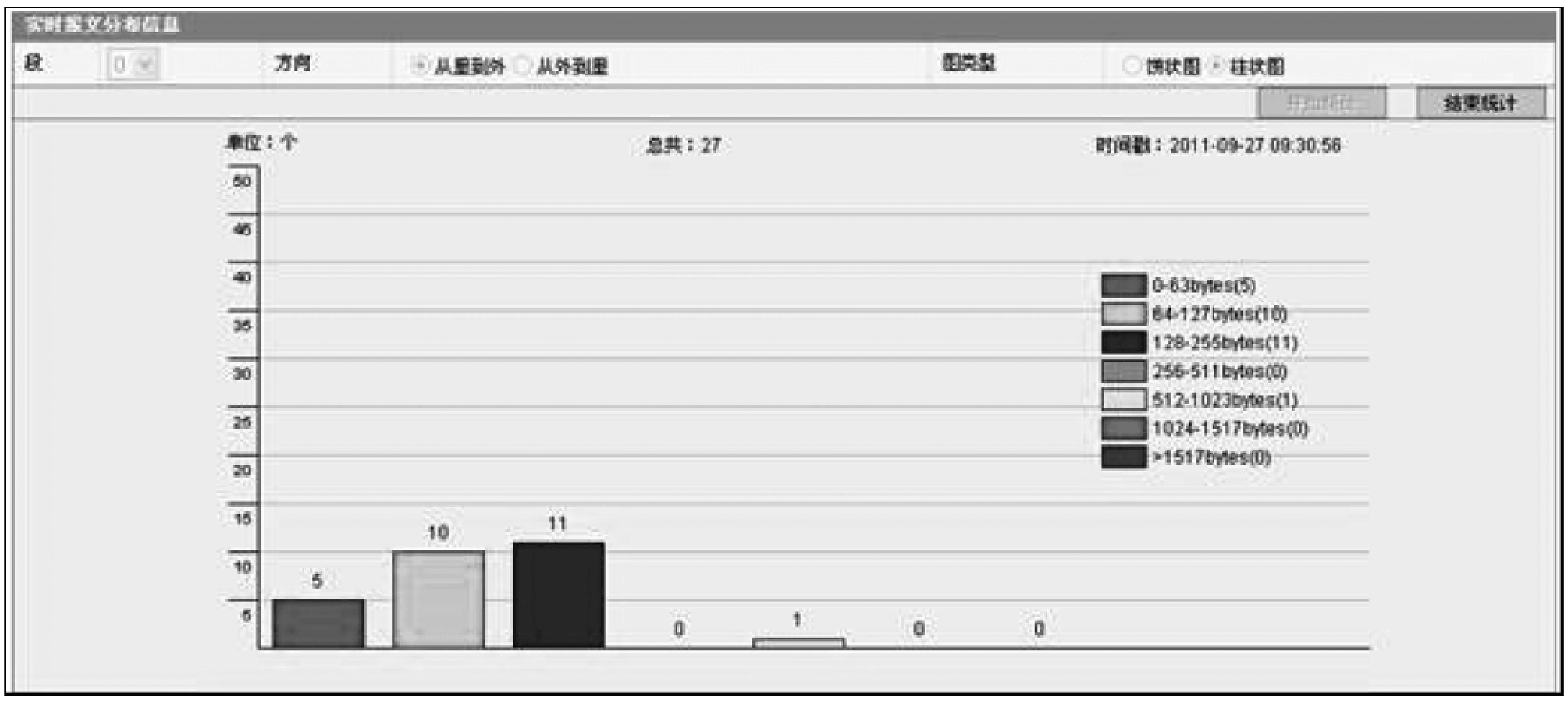


图 6-218 实时报文统计

②“仔细看”。在导航栏中单击“带宽管理”→“策略管理”,新建策略应用,默认规则工作选择“permit+notify”,通过带宽管理检测所有流量应用。在日志中过滤出想要的五元组日志,如图 6-219 所示,可以看到访问网站的流量是否双向被检测到,如果检测到则说明双向引流成功。



图 6-219 新建策略应用

（5）查看带宽管理配置

查看 ACG 带宽管理全局配置，确认多条策略无地址重复调用。

例如：通过查看 ACG 的 Web 页面，查看带宽策略调用地址情况，如图 6-220 所示。



图 6-220　带宽策略调用地址

如图 6-220 所示，ACG 带宽管理策略中，无地址重复调用情况，仅策略名称为迅雷 1 的策略生效，应用于段 0 上。

查看 ACG 带宽管理配置，确认配置了基于应用的策略。

例如：通过 ACG 的 Web 页面，查看设备带宽管理的配置，确认设备配置了正确的应用配置，如图 6-221 所示。



图 6-221　带宽管理策略应用

如图 6-221 所示，迅雷 1 的带宽管理策略中，配置了限制迅雷的规则，动作集为 Block＋Notify，应用在段 0 上，匹配内部和外部所有 IP。

（6）判断是否为误识别

在上述信息均确认无误的情况下，通过配置测试 IP，进行信息收集。

收集方法如下。

① 配置测试 IP，如本机测试 IP 地址并应用于段策略中，如图 6-222 和图 6-223 所示。

② 策略中规则动作配置为 permit＋notify，如图 6-224 所示。

③ 策略激活后，进行需要限制的业务访问，导出服务日志，如图 6-225 所示。

④ 记录设备特征库版本信息，如图 6-226 所示。

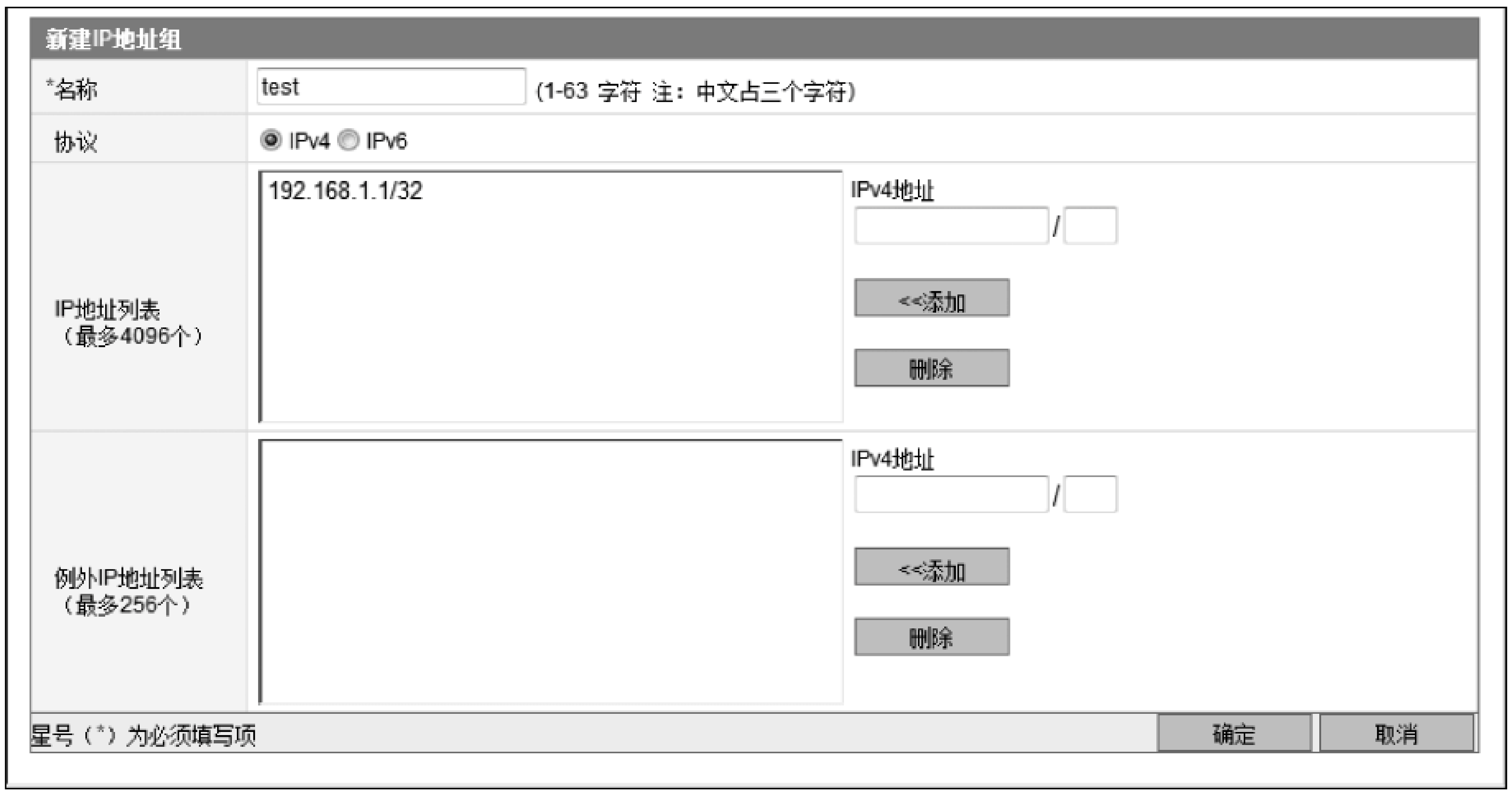


图 6-222 新建 IP 地址组



图 6-223 策略应用范围



图 6-224 规则配置



图 6-225 服务日志查询



图 6-226 当前版本

⑤ 记录设备 License 信息，如图 6-227 所示。

License信息

特征库	有效日期
APP	2012-03-02

特性	有效日期	状态

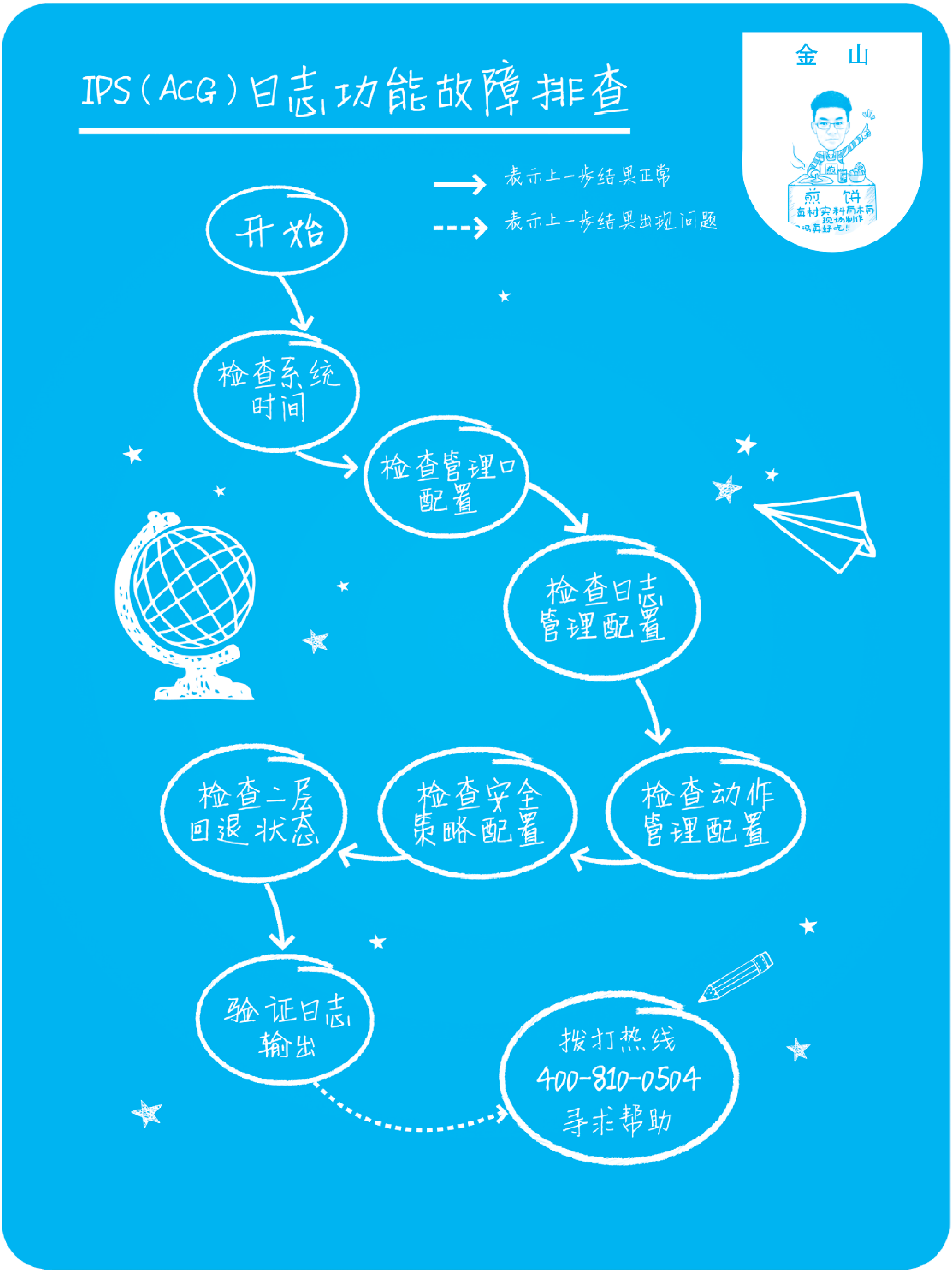
图 6-227　License 信息

⑥ 记录所使用软件版本，如迅雷，如图 6-228 所示。



图 6-228　迅雷

记录输出后，一并反馈总部处理。


IPS(ACG)日志功能故障排查
金 山
煎 饼
表示上一步结果正常
表示上一步结果出现问题
开始
检查系统时间
检查管理口配置
检查日志管理配置
检查动作管理配置
检查安全策略配置
检查二层回退状态
验证日志输出
拨打热线
400-810-0504
寻求帮助

1. 开始

IPS(ACG)日志功能问题定位故障的思路是：首先检查系统时间是否正确，然后检查与日志功能相关的各项配置是否正确，然后检查系统工作状态是否正确，最后通过搭建日志主机等方式验证设备日志功能是否正常。

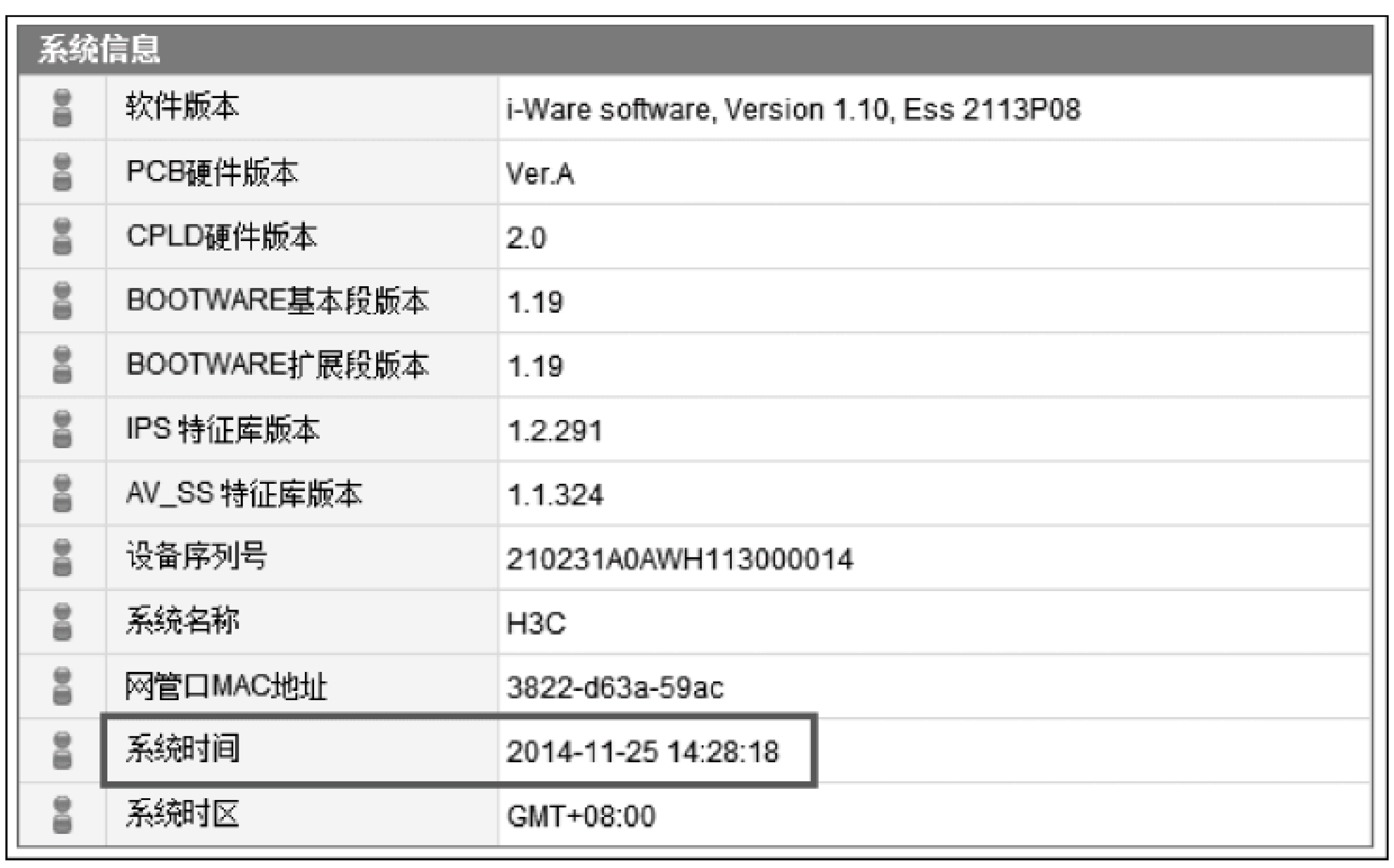
2. 流程图相关操作说明

(1) 检查系统时间

查看设备当前时间是否正确。因为 IPS(ACG)产生各类日志时将以系统时间为基准添加时间戳，因此如果系统时间不正确，将使设备日志查询模块或日志服务器无法根据当前的实际时间将日志展示出来。盒式设备的系统时间可由管理员手工配置，也可通过指定 NTP 服务器进行同步，注意应当为设备配置正确的时区，中国国内为东八区；插卡式设备的系统时间是通过 ACSEI 协议与路由交换主机进行同步的，因此需要为路由交换主机配置正确的系统时间和时区，同样推荐使用 NTP 协议来实现时钟同步。

当 IPS(ACG)与 H3C SecCenter 配合使用时，推荐设备及安装 SecCenter 的服务器操作系统均配置为东八区，并与 Internet 上的 NTP 服务器保持时钟同步。此时在 SecCenter 上添加 IPS(ACG)的设备访问参数中，时间纠正方式必须选择“以本地时间处理”。

例如：可以在设备 Web 管理页面“系统管理→设备管理→系统信息”中查看到 IPS(ACG)设备的当前时间，如图 6-229 所示。



系统信息	
软件版本	i-Ware software, Version 1.10, Ess 2113P08
PCB硬件版本	Ver.A
CPLD硬件版本	2.0
BOOTWARE基本段版本	1.19
BOOTWARE扩展段版本	1.19
IPS 特征库版本	1.2.291
AV_SS 特征库版本	1.1.324
设备序列号	210231A0AWH113000014
系统名称	H3C
网管口MAC地址	3822-d63a-59ac
系统时间	2014-11-25 14:28:18
系统时区	GMT+08:00

图 6-229　系统信息

(2) 检查管理口配置

IPS(ACG)设备必须通过管理口才能将日志报文发送至远程日志主机上，因此需要保证管理口配置正确，设备指向网管服务器/远程日志主机的路由正确，管理端口工作状态正常。盒式设备默认路由应当指向管理端口所在网段的网关设备；插卡式设备默认路由应当指向前面板口所在网段的网关设备，即不允许通过插卡与路由交换主机的内联口作为管理设备和日志发送的通道，必须使用插卡前面板口。注意同时检查与管理口互联的对端设备接口工作状

态是否正常，速率双工是否一致，收发数据报文是否存在错包等。

例如：可以在设备 Web 管理页面“系统管理→网络管理→管理口”中查看到 IPS(ACG)设备的管理端口地址/掩码、路由配置。该设备的管理端口为 meth0/2，管理 IP 地址为172.31.0.14，配置的网关为 172.31.0.1，分别如图 6-230 和图 6-231 所示。

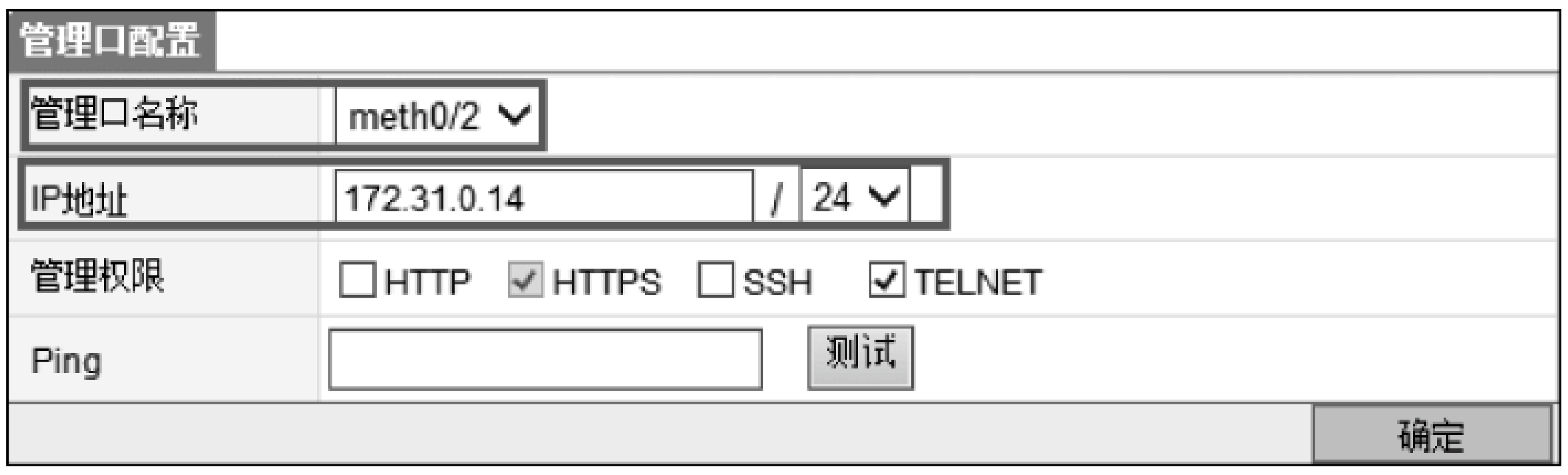


图 6-230　管理口配置

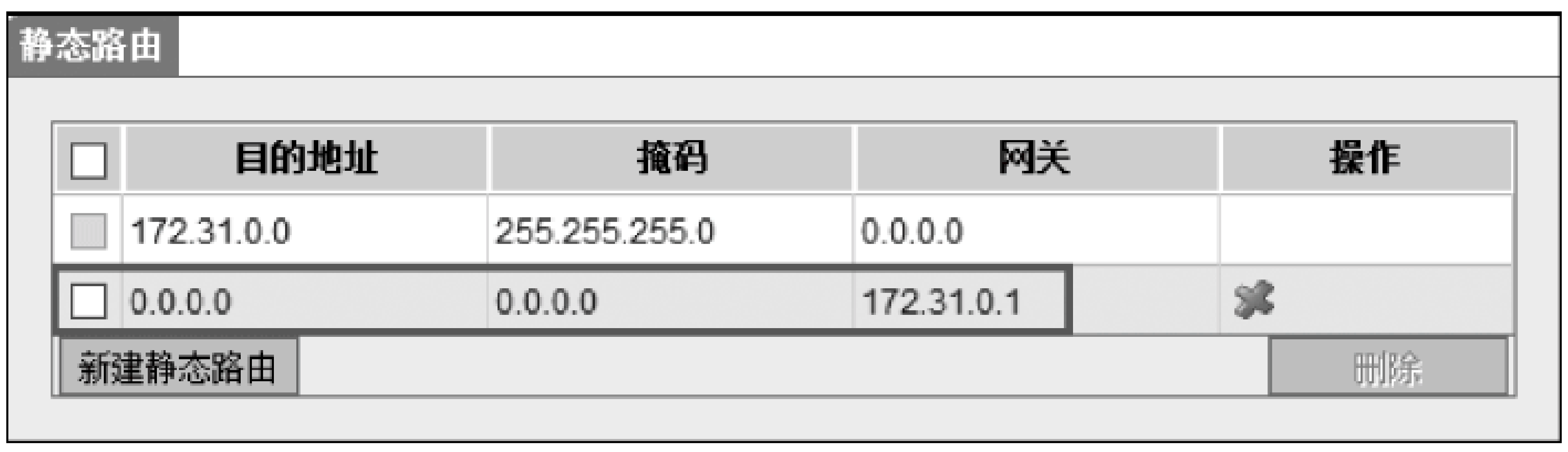


图 6-231　静态路由

例如：可以在设备 Web 管理页面“系统管理→网络管理→接口配置”中查看到 IPS(ACG)设备的管理端口连接正常，当前状态为 1000Mbps 全双工，如图 6-232 所示。



图 6-232　接口配置

(3) 检查日志管理配置

IPS(ACG)系统的日志配置模块用于对各种日志的保存和输出参数进行配置，具体包括“配置设备日志”和“配置数据日志”两部分。前者用于配置系统日志和操作日志的本地保存/远程输出相关参数，后者用于配置数据日志的最大保存天数、Syslog 主机、发送日志 E-mail 和邮件服务器的相关参数。

设备日志主要包含系统日志和操作日志，分别为设备运行过程中有关自身状态的日志信息和管理员在设备上执行各类操作的相关日志信息。当与 H3C SecCenter 配合时，由于其默认的安全设备 Syslog 接口端口为 UDP 30514，因此在检查配置时需注意设备发送端口配置是否和日志服务器接收端口一致。如果希望在设备本地查看相关日志，需注意由于硬件存储空间十分有限，当设备存储日志占用的存储空间超过了设置的阈值后，系统将自动删除最老的日志文件，同理，系统也会自动删除超过了“本地日志最大保存天数”的日志文件。可以通过删除

无用的版本文件和设置较长的日志保存天数，使 IPS(ACG)本地存储更多的日志。

例如：可以在设备 Web 管理页面“日志管理→日志配置→设备日志”中，查看 IPS(ACG)设备已经开启发达系统日志及操作日志，如图 6-233 所示，指定的日志服务器地址为 172.30.255.200，目的端口为 30514。

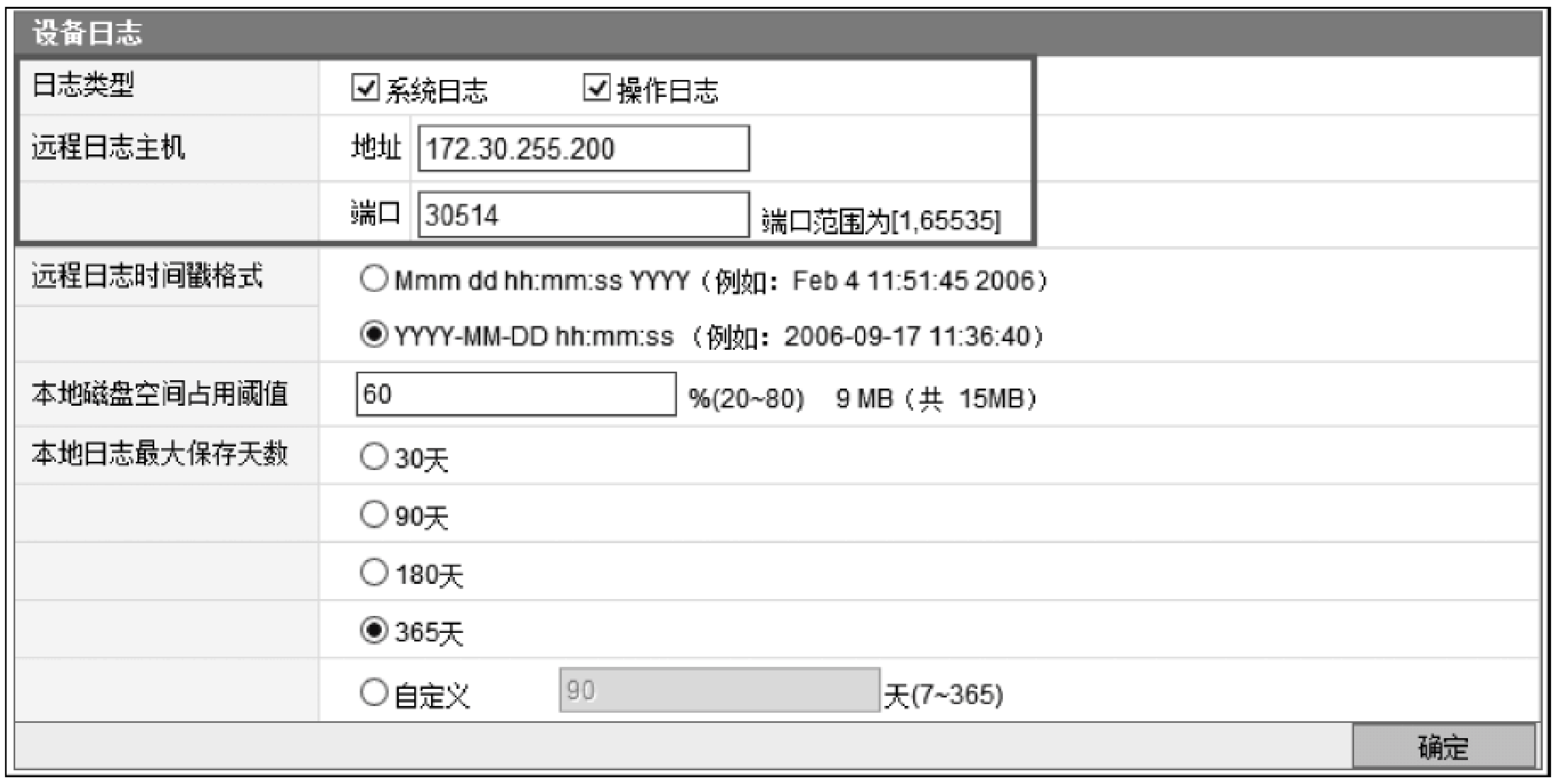


图 6-233　设备日志

数据日志是指 IPS 攻击防范日志、AV 防病毒日志、带宽管理服务日志、URL 过滤日志等安全策略相关的日志。需准确配置 Syslog 主机的 IP 地址和端口号，设备才能将产生的数据日志输出到指定的远程日志主机。当与 H3C SecCenter 配合时，由于其默认的安全设备 Syslog 接口端口为 UDP 30514。IPS(ACG)本地数据库中能保存的数据日志条数有一定的限制，超过限制后系统会自动从最老的日志开始删除数据日志的 10%。

例如：可以在设备 Web 管理页面“日志管理→日志配置→数据日志”中查看到 IPS(ACG)设备数据日志的最大保存天数、Syslog 主机配置等，如图 6-234 所示。

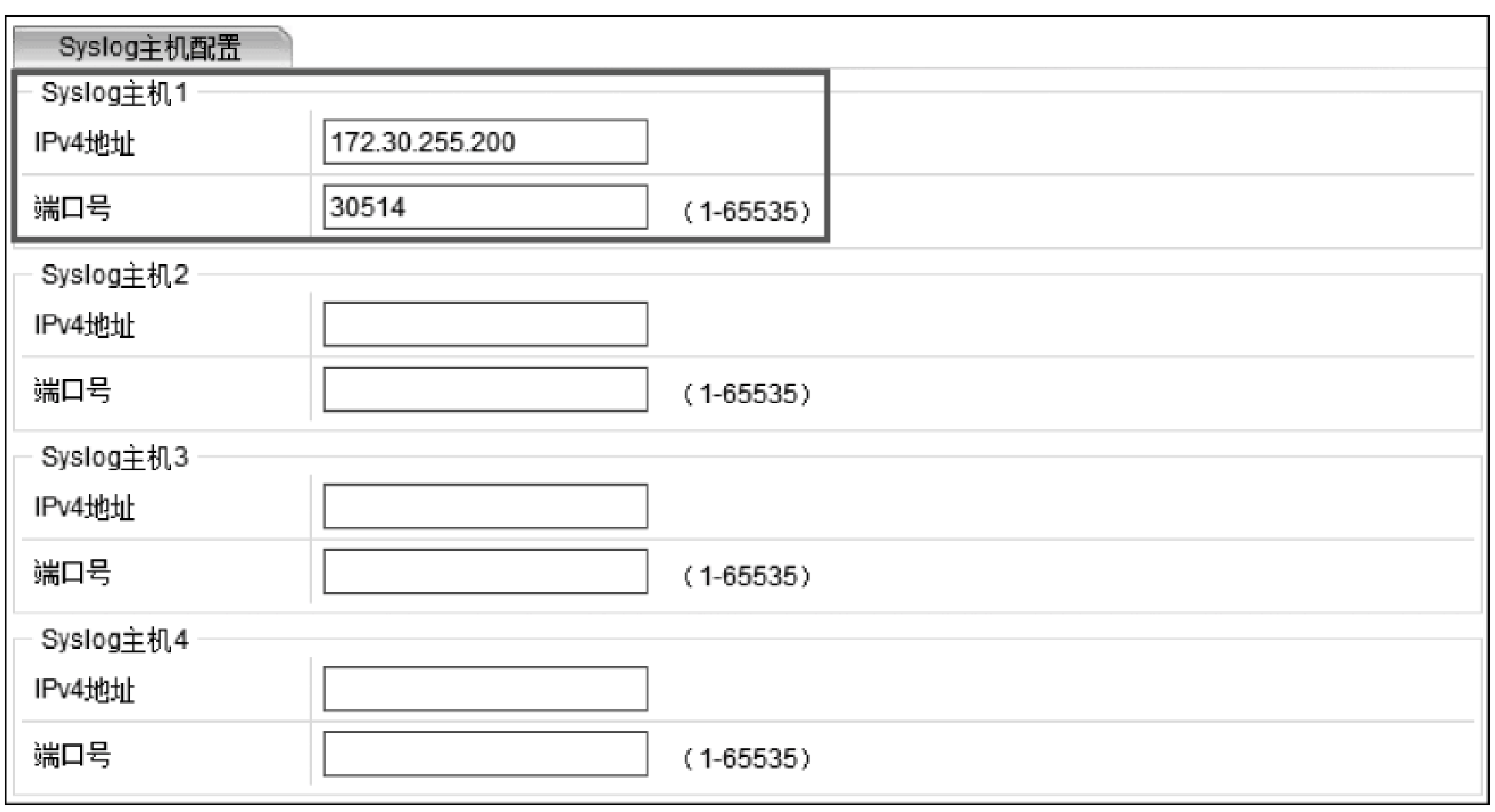


图 6-234　Syslog 主机配置

(4) 检查动作管理配置

IPS(ACG)动作管理模块用于对动作和动作集的管理。动作集是一组动作的集合，可以

被 IPS 攻击防范策略、AV 防病毒策略、带宽管理策略、URL 过滤策略等安全策略引用，可设置对命中策略的业务流量所采取的动作。动作包括阻断动作、通知动作和报文跟踪上传动作三类，与 IPS(ACG)日志功能有关的是通知动作。通知动作包括三种具体的方式：E-mail 通知、输出到本地数据库、输出到 Syslog 主机。当需要直接在 IPS(ACG)设备上查看各安全策略产生的日志时，须使用输出到本地数据库方式；当需要与远程日志服务器如 H3C SecCenter 配合时，须使用输出到 Syslog 主机方式。通知动作可以被引用至动作集中，动作集可以被 IPS(ACG)的各类安全策略引用，指导设备按客户需求产生和输出日志。

系统预定义的“Notify”动作默认仅定义了通知到数据库，即把日志保存在设备本地。如果希望将日志发送给远程主机，可添加通知到 syslog 主机参数，也可由管理员新建一个包含通知到 syslog 主机参数的自定义通知动作。

例如：可以在设备 Web 管理页面“系统管理→动作管理→通知动作列表”中查看到预定义和自定义的通知动作。如图 6-235 所示，可以看到系统预定义的 Notity 通知动作仅使能了输出到本地数据库属性。



图 6-235　通知动作

(5) 检查安全策略配置

IPS(ACG)产品支持攻击防范策略、病毒防范策略、带宽管理等多种安全策略，通过将策略应用在段上以实现 IPS(ACG)的各种安全特性。除了在前述几个步骤中的必要配置外，在各个安全策略中，关于日志输出部分可能有部分额外配置点需要检查；否则，仅需在段策略上配置规则并引用包含通知动作的动作集即可。各安全策略具体配置方法可查阅产品用户手册和 Web 配置指导手册。特别需注意：当安全策略应用至段后，必须通过单击“激活”按钮并返回操作成功提示后才会真正生效。

例如：当网络管理员部署 IPS 攻击防范策略且需将产生的日志发送到远程日志主机时，应在设备 Web 管理页面“IPS→高级配置”中选中“输出到 Syslog 主机”复选框，如图 6-236 所示。

然后在设备 Web 管理页面“IPS→策略管理”中，确保应用在段上的攻击防范策略规则中引用了包含相应通知动作的动作集，如图 6-237 所示。



图 6-236　高级配置



图 6-237　新建策略应用

例如：当网络管理员部署 URL 过滤策略且需将产生的日志发送到远程日志主机时，应在设备 Web 管理页面“URL 过滤→全局配置”中，选中高级设置中的“输出到 Syslog 主机”复选框，如图 6-238 所示。

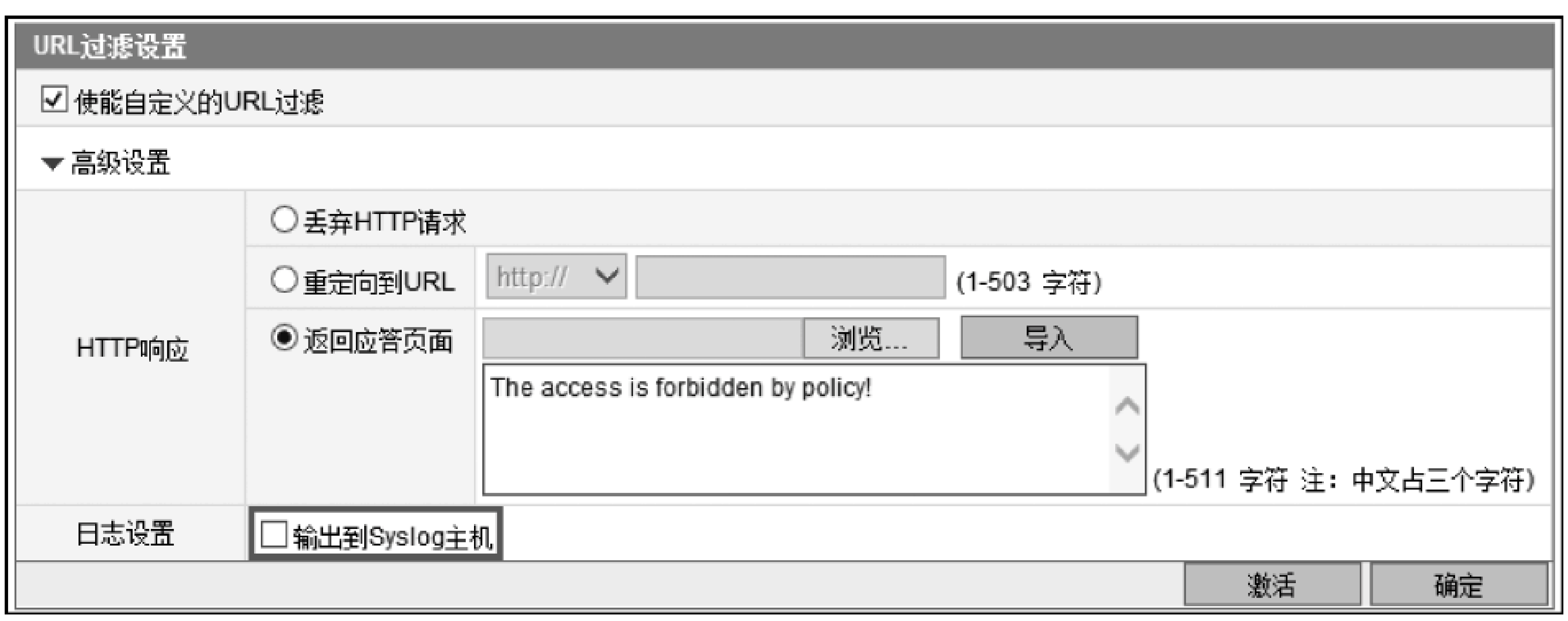


图 6-238　URL 过滤设置

(6) 检查二层回退状态

IPS(ACG)产品内置的软件监测模块以很高的频率实时检查设备自身的健康状况。一旦

该模块发现检测引擎、软件系统出现故障或业务流量太大超过了设备处理性能以致大量丢包时，会立即将设备设置成一个简单的二层交换模式。此时，设备对端口接收的所有流量不再执行任何检测，而是直接将内外部域贯通，保证网络业务的连续性，该功能简称为“二层回退”。当设备进入“二层回退”状态后，所有软件功能不再生效，也不再产生任何数据日志信息，因此需要检查当前设备是否已经人为操作或自动开启了“二层回退”。

例如：可在设备 Web 管理页面“系统管理→高可靠性→二层回退”中，查看设备当前二层回退状态为绿色时，表示工作正常；若状态灯为红色，则说明此时设备已经进入二层回退状态，如图 6-239 所示。

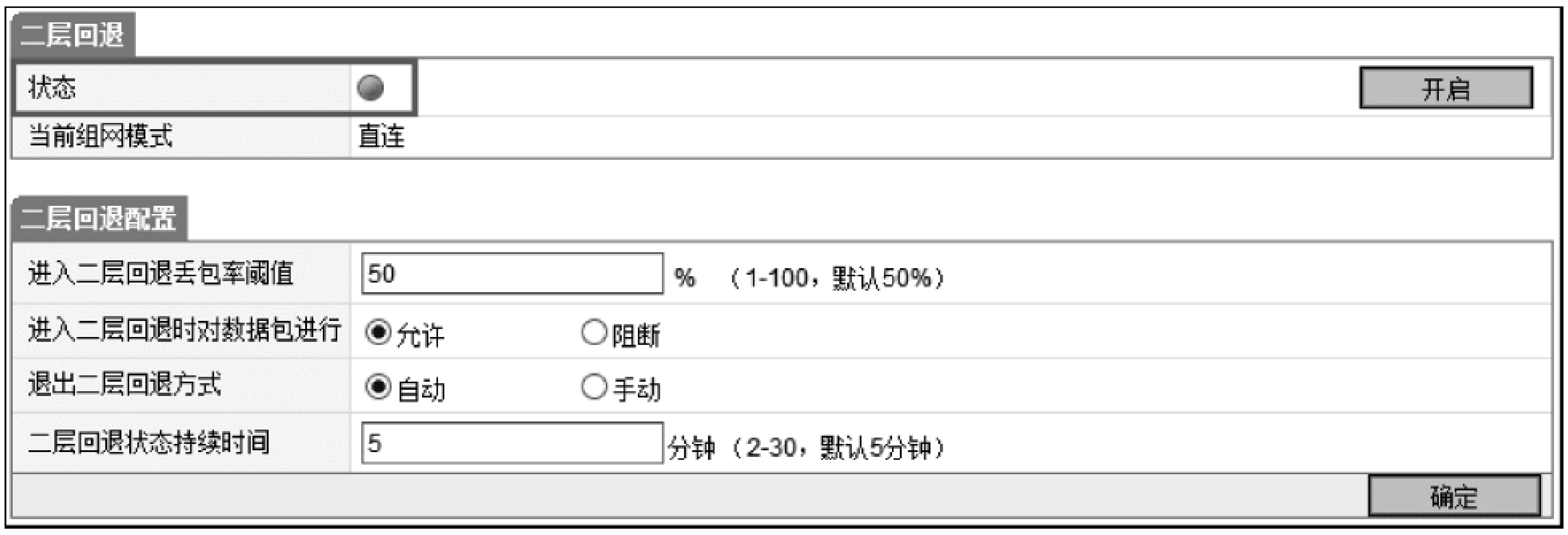


图 6-239　二层回退状态

(7) 验证日志输出

在 IPS(ACG)产品配置界面中完成所有与日志输出相关的配置检查后，对于系统日志、操作日志、通知到数据库的数据日志信息，可直接在 Web 管理界面的日志管理中分类查询；对于通知到 Syslog 主机的数据日志信息，可在远程日志服务器(如 H3C SecCenter)上查询。

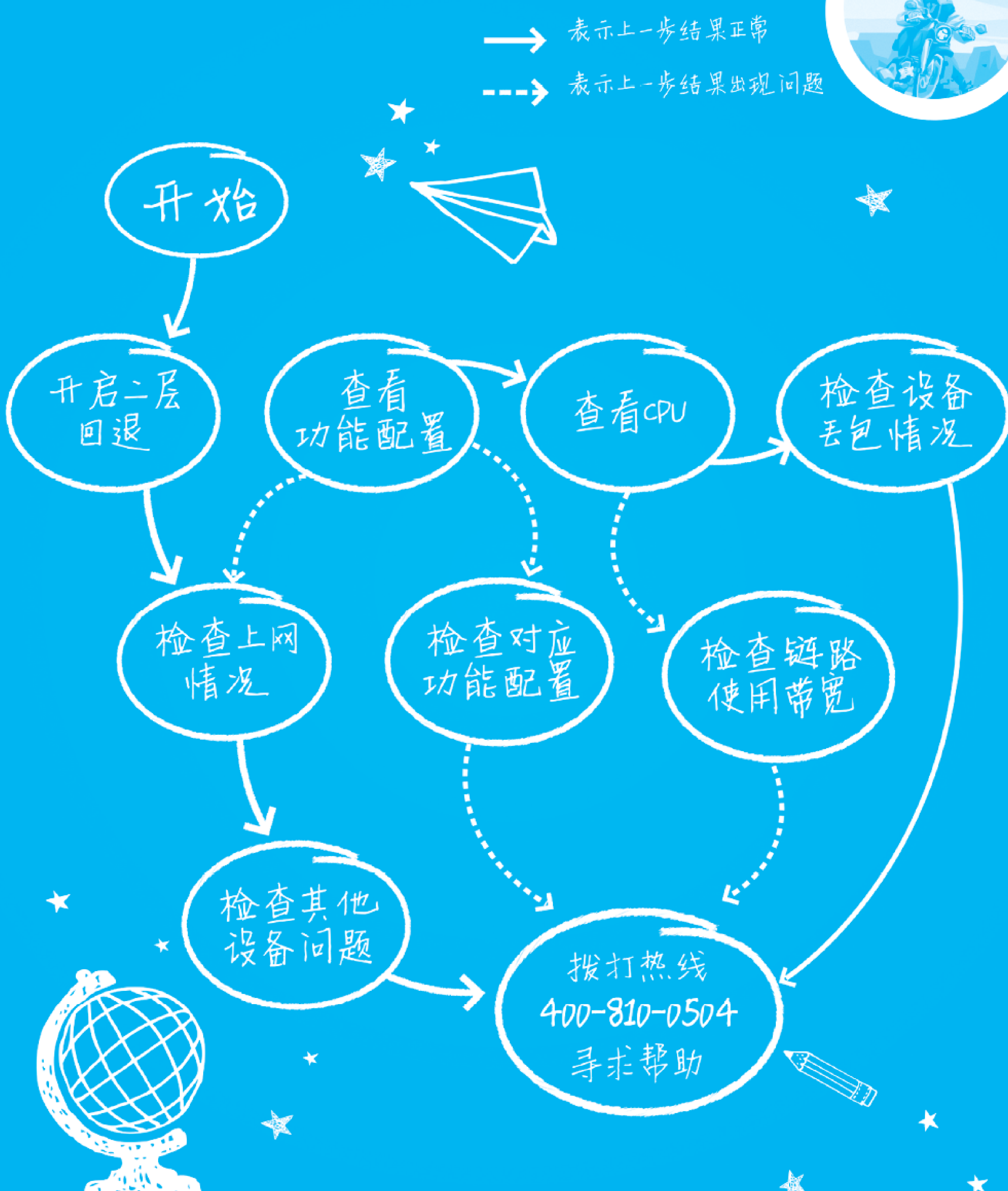
当查询不成功，无法找到相应的日志时，注意检查设备本地存储空间是否已满，日志主机数据库系统的安装磁盘是否还有剩余空间、数据库自身状态是否正常、设备日志发送端口与服务器接收端口是否一致，等等。

IPS(ACG)产品将日志发送至 Syslog 日志主机需经过中间设备，因此还要检查 IPS(ACG)管理端口与服务器端口之间是否 IP 可达，管理报文及日志报文是否正常转发未被其他设备错误丢弃。可在 IPS(ACG)设备上将 PC 机 IP 地址设置为 Syslog 主机地址，然后在 PC 机上利用抓包软件来判断设备是否可以正常发送日志报文。

IPS（ACG）上网慢故障排查

莘启跃





06 安全产品 > 6.3 LB > 6.3.11 IPS(ACG)上网慢故障排查 > 步骤详解

1. 开始

IPS(ACG)使用我司的 i-Ware 平台，主要配置基于 Web，检测对象为 4～7 层业务，出现问题多样化，排查思路也不同。

IPS(ACG)上网慢问题定位故障的思路是：通过二层回退来判断上网变慢是否是 IPS(ACG)造成的。如果不是则排查其他设备，如果是则通过在设备上收集信息来一步步排查具体的原因。

2. 流程图相关操作说明

(1) 开启二层回退

设备内置的监测模块以很高的频率定时地监测自身的健康状况，一旦探测到检测引擎、软件系统故障或者流量过大时，该模块会将设备设置成一个简单的二层交换设备。此时，设备对所有网络流量都不进行检测，网络流量将在两个接口之间直接贯通，从而保持网络业务的连续性。这个功能称为"二层回退"。

设备还支持用户手动设置设备进入/退出二层回退状态。

举例：在导航栏中单击"系统管理→高可靠性→二层回退"，进入二层回退的配置页面，如图 6-240 所示。



图 6-240　二层回退配置

(2) 查看上网情况

手动开启"二层回退"之后，再通过设备上网测试开启二层回退前后上网快慢是否有明显变化。

当运行正常的网络突然出现问题时，要排除是否是 IPS(ACG)引起，最简单有效的方法就是将 IPS(ACG)二层回退。如果二层回退之后问题仍然存在，请排查其他设备；如果问题不存在了，说明问题出在 IPS(ACG)上，再具体问题具体分析。

(3) 检查其他设备问题

如果"二层回退"开启后问题不存在，则很大可能性是其他设备的问题。浏览网页慢可以通过"HTTP WATCH"等软件来抓取交互过程，分析哪一步延迟较大。如果是其他应用程序感觉网络传输较慢，可以通过在终端侧抓包来判断是否有丢包或者重传。

如果未发现其他设备问题，为了最终确认是不是 IPS(ACG)问题，可以收集设备诊断、系统日志，操作日志，设备系统状态截图，系统信息截图反馈给 400 进一步分析。

(4) 查看功能配置

造成上网慢或者异常的功能有以下几种：带宽管理功能、QoS 通道限速功能、URL 过滤功能、防攻击/防病毒功能。

为了判断是否是功能配置问题，可以依次关闭某个功能策略，判断哪一个策略能解决问题。如果没有解决，则排除配置问题。

举例：关闭“通道带宽管理”功能，发现上网慢问题解决，则可判断是此功能引起的问题。

(5) 检查对应功能配置

确定某个功能导致上网慢后，可以根据功能配置指导和注意事项来排查，下面简单介绍这些功能有可能造成上网慢的原因。

① 带宽管理[IPS(ACG)]。网络流量按照其用途的不同划分成不同的服务类型，例如 E-mail 服务、VoIP 服务等，对不同的服务类型实施不同的管理控制行为，称为带宽管理。

带宽管理通过对各种应用进行灵活的带宽控制，限制非关键应用，并保证了客户网络上关键应用的带宽。

容易造成“上网慢”的原因可能是做了限速或者阻断，还有一种原因是误识别。

若在带宽管理策略中发现做了限速或者阻断，可根据客户要求调整速率上限或者完全放通；若在策略中未发现问题应用对应的限速或者阻断，则可以通过日志来判断是否存在误识别，比如看视频慢时是否每次都看到日志记录限速或阻断了 P2P 下载，这样的话可能设备将视频应用误识别为 P2P 应用了。此种情况可以在客户端抓包，收集设备版本信息和特征库版本信息给 400 进行分析，必要时更新特征库。

举例：图 6-241 为带宽管理配置界面(“带宽管理→策略管理”)，需要注意应用控制对应的动作集。

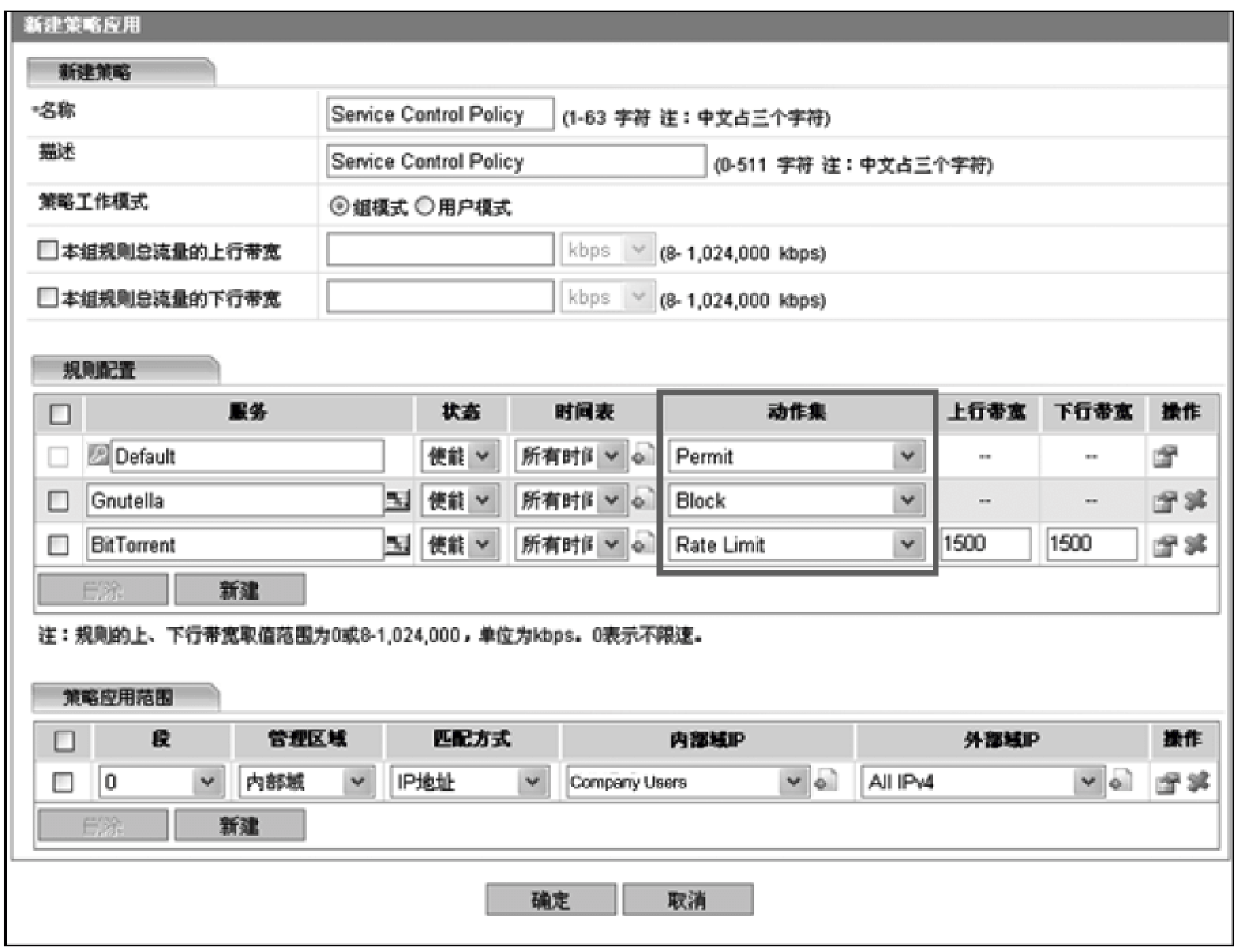


图 6-241 带宽管理配置

② 通道带宽管理(ACG)。通道带宽管理技术根据不同的段、用户、应用或业务分层次的划分出多条不同的通道，对这些通道分别进行带宽控制以及各种精细化地动作管理。

通道带宽管理也会存在误识别的情况，如果针对某个应用发现有误识别同样需要反馈客

户端抓包，收集设备版本信息和特征库版本信息给总部进行分析。对于限速行为导致的上网慢，可以调整策略配置。

例如：在“通道带宽管理”→“通道策略”里可以看到配置的策略，注意服务类型和通道带宽设置，如图 6-242 所示。



图 6-242　通道策略配置

③ URL 过滤[IPS(ACG)]。URL 过滤是一种网页过滤功能，支持自定义 URL 过滤。

对于某类网站打不开的情形，可以查看设备是否配置了 URL 阻断，命中了 URL 策略。

例如：图 6-243 为 URL 过滤规则配置界面，需要检查阻断时间，是否在问题时间段内上网被阻断。

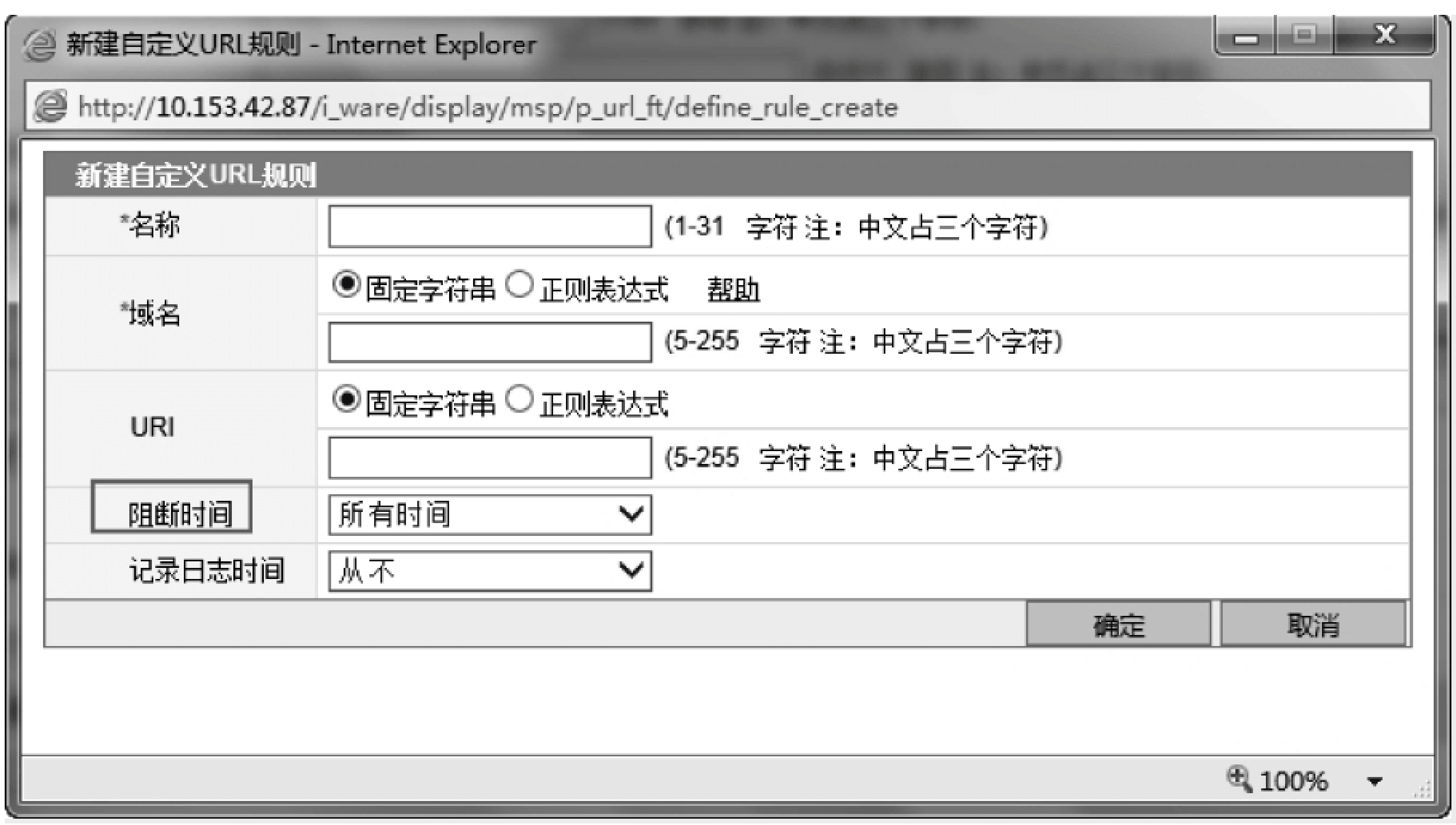


图 6-243　URL 过滤规则配置

④ IPS/防病毒(IPS)。如果访问的网站或者应用含有攻击流量或者病毒，在开启 IPS/防病毒的情况下也会对其进行阻断，用户不知情会认为上网出现异常。不排除 IPS/防病毒检测存在误识别的情况，此时需要查看日志信息，判断用户上网行为被误判成何种攻击或者病毒，反馈客户端抓包、设备版本和特征库版本。

例如：在“日志管理→攻击日志→最近日志”中可以查看到设备攻击日志，可以用来判断访问的目的 IP 是否被 IPS 阻断，如图 6-244 所示。



	攻击ID	时间	攻击名称	段	方向	源IP	目的IP	源端口	目的端口	应用协议	级别	Packet Trace
1	151001842	2009-07-18 15:56:55	Microsoft Windows SMB WINREG 信息收集	0	从外到里	10.0.0.11	10.0.0.12	1078	445	netbios-ssn (TCP)	提示	fff
2	151001842	2009-07-18 15:56:52	Microsoft Windows SMB WINREG 信息收集	0	从外到里	10.0.0.9	10.0.0.10	1078	445	netbios-ssn (TCP)	提示	fff
3	151001842	2009-07-18 15:56:49	Microsoft Windows SMB WINREG 信息收集	0	从外到里	10.0.0.7	10.0.0.8	1078	445	netbios-ssn (TCP)	提示	fff

图 6-244　设备攻击日志

(6) 查看 CPU

通过查看 IPS(ACG)数据面 CPU 高低可以知道问题原因是否和 CPU 过高所致。

如果发现多数 CPU 核统计值接近 100%,则怀疑网络流量达到设备性能。

还有一种情形则是一个或者几个 CPU 比较高,这种情况可能是由于分流不均或者单个 IP 地址流量过大导致。

① 分流不均。检查设备部署位置,是否在 NAT 设备之后,或者处于隧道中间,经过 IPS(ACG)的流量如果经过了 NAT 转换或携带隧道信息,会因为源 IP 地址过少,导致分流不均,单个 CPU 利用率过高,继而丢包。有时候内外部域接反了,外网 IP 相对较少时,也会出现分流不均的情况。

确认分流不均后,可以根据实际情况调整设备部署位置,或者重新连线。

② 单个 IP 地址流量过大。一般情况下,需要结合流量报表进行确认。在流量报表上查看流量最大的 IP 地址、该 IP 地址对应的流量类型,有可能是大量 P2P 下载,有可能是被攻击或者中病毒后对外发起攻击或其他可能的情况。

确定 IP 地址后,可以将该 IP 地址暂时封杀,如加入黑名单或对该 IP 限速。恢复网络后再针对具体 IP 分析。

命令:shell 视图下(shell 视图进入方式可拨打 400 热线咨询)

[H3C-hidden-expend]cat /proc/iware_os/cpu_sec

例如:如下所示少量 CPU 核达到 100%,可判断存在分流不均或者单个 IP 地址流量过大的可能性。

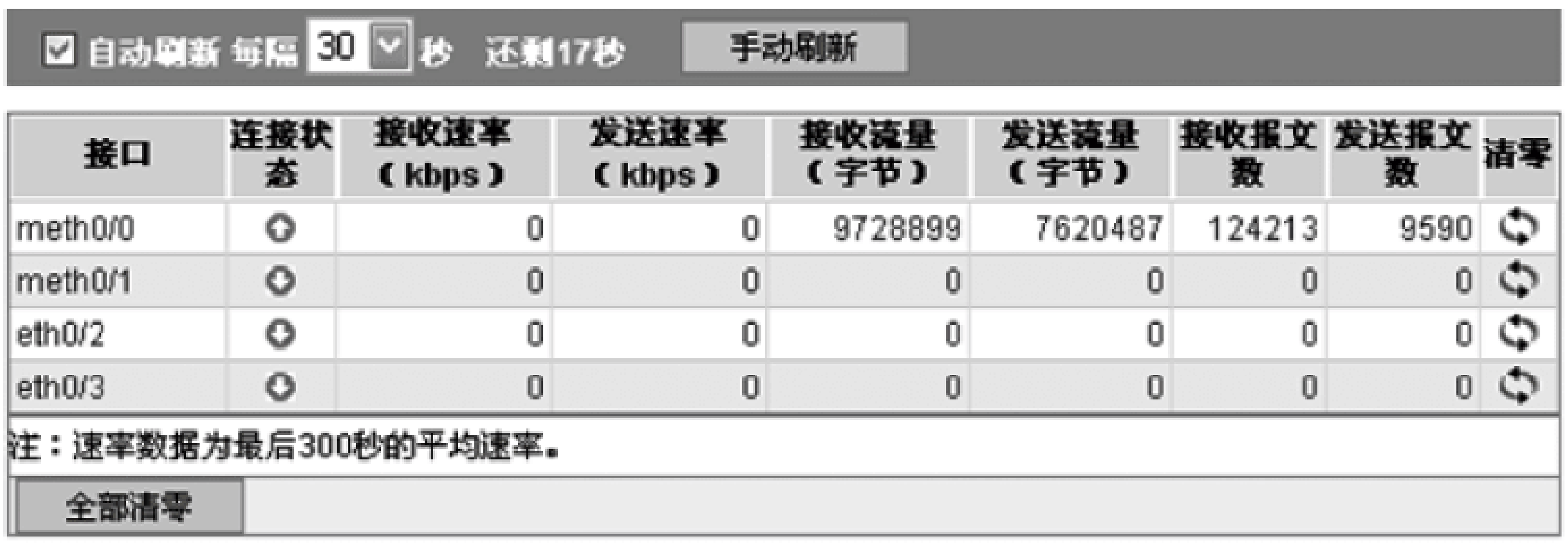
```
[H3C-hidden-expend]cat /proc/iware_os/cpu_sec
3
100
0
0
0
0
100
0
100
0
0
…
```

（7）检查链路使用带宽

前面查看了数据面 CPU 情况，如果多数 CPU 核数值较高，甚至接近 100%，可以怀疑是设备性能原因。

为了确定此种情况，需要查看链路带宽占用情况。如果占用较多，甚至接近接口承载带宽，则说明流量确实达到设备性能，想要解决，需要更换升级设备。

例如：在导航栏中单击“系统管理”→“网络管理”→“接口流量”，进入如图 6-245 所示的页面，可以查看设备上各接口的流量信息。



自动刷新 每隔 30 秒 还剩17秒 手动刷新

接口	连接状态	接收速率（kbps）	发送速率（kbps）	接收流量（字节）	发送流量（字节）	接收报文数	发送报文数	清零
meth0/0		0	0	9728899	7620487	124213	9590	
meth0/1		0	0	0	0	0	0	
eth0/2		0	0	0	0	0	0	
eth0/3		0	0	0	0	0	0	

注：速率数据为最后300秒的平均速率。

全部清零

图 6-245　接口流量

如果出现数据面 CPU 近 100%，网络流量占用带宽接近接口满值，则认为转发量达到设备性能。

如果出现数据面 CPU 近 100%，但是网络流量并不大的情况，一种很大的可能性就是特征库中某条特征被频繁命中，导致性能急剧下降。确认是否频繁命中特征，可在系统视图下，使用 display dip 命令查看特征命中情况。

命令：[H3C]*display dip*

[H3C]*dip clean*

例如：判断是否是特征库中某条特征被频繁命中，请先将 dip 信息清除，系统视图下输入 dip clean。

命令：[H3C]*dip clean*

然后再多次查看 display dip 的信息。

```
[H3C]display dip
Signature   AC Hit   1st Try   More Try   PCRE Hit   Rule Hit   Expire
67112926    3202     0         0          0          0          0
151002748   10951    10951     0          0          0          0
151002956   5055     5055      0          0          0
```

当出现某条特征对应的 AC HIT 统计特别大，并且变化非常快时，说明该条特征被频繁命中。如例子中所示，151 开头的特征是 IPS 攻击规则对应的 ID 号，可以直接根据该 ID 号在 Web 上查询是哪条规则被频繁命中，查询完成后，可直接禁止该规则。

而以 6 开头的特征一般是服务特征，具体对应哪种服务类型需要查数据库，建议将 display dip 信息收集回来处理。

特征被频繁命中，一般是因为特征定义不够严格，或者网络中本身存在大量匹配我司特征库的流量。出现这种情况时，请提供 display dip 完整收集信息，并对网络流量进行抓包，反馈处理。后继可通过升级特征库解决。

需要注意的是，dip 相关命令不可见，且不支持联想及↑↓键查询，需要每次手工输入。

（8）检查设备丢包情况

设备如果发生硬件丢包，可以通过如下命令查看。

命令：shell 视图下（shell 视图进入方式可拨打 400 热线咨询）

[*H3C-hidden-expend*]*iftable_display*

[*H3C-hidden-expend*]*dmesg -c*

例如：在 shell 视图下，执行 iftable_display 命令，再用 dmesg -c 命令查看统计，需要多执行几次。中间可用命令 iftable_display clear 先清除统计信息，再重新查看。

```
[H3C-hidden-expend]iftable_display
[H3C-hidden-expend]dmesg -c
...
display interface information:
 ifindex,    recv_error,      queue_drop,      to_iware,     send_fail
      4,             0,               0,              0,     1548672,
 dpvirt   : trunkid_p[2bd17000], trunkinfo_p[2bd19000]
 phys     : trunkid_p[3bd17000], trunkinfo_p[3bd19000]

NA buffer information:
 XLR_IO_DEV_GMAC_ARxDescInMAC      2000   FifoCount    2000
 XLR_IO_DEV_XGMAC_ARxDescInMAC    30720   FifoCount   30720
 ...
```

参数 display interface information 中，queue_drop，recv_error，send_fail 存在统计，并不断增长，因此认为设备有丢包。除了反馈上一步信息外，请收集设备诊断信息、系统日志、操作日志、设备状态信息和接口信息。

07

无 线 产 品

陈 铮


表示上一步结果正常
表示上一步结果出现问题
开始
查看当前设备CPU状态
查看各进程占用CPU情况
无线设备CPU利用率高故障排查
了解当前网络是否存在重大操作
反馈具体操作收集信息
收集信息
拨打热线 400-810-0504寻求帮助

07 无线产品 > 7.1 AC > 7.1.1 无线设备 CPU 利用率高故障排查 > 步骤详解

1. 开始

CPU 超负荷运行时会造成很多问题，此时设备会出现丢包现象，从而导致正常业务受到很大的影响。

定位故障的思路如下。

① 判断当前 CPU 是否正常。

② 判断近期操作是否影响到 CPU。

③ 判断具体是哪个进程长时间占用 CPU。

2. 流程图相关操作说明

(1) 查看当前设备 CPU 状态

查看当前设备 CPU 信息是否正常，以便明确下一步操作。

命令：*display cpu-usage*

例如：通过命令查看，可以确认当前 CPU 是否处于正常状态(长期高于 70%表示异常)。

```
<AC>display cpu-usage
Unit CPU usage:
        70% in last 5 seconds
        71% in last 1 minute
        75% in last 5 minutes
```

(2) 查看各进程占用 CPU 情况

命令：进入隐藏模式。

display cpu-usage task

reset task-runtime-max

display task

例如：通过命令查看，可以确认具体是哪些进程大量占用 CPU，表 7-1 列出了常见 CPU 进程具体含义。

表 7-1 常见 CPU 进程具体含义

进 程 名 称	具 体 含 义	常见问题触发原因
VIDL	空闲状态	表示当前 CPU 处于空闲状态的百分比
INFO	信息中心模块	开启过多的 debugging 信息等原因触发
ARP	ARP 相关模块	开启 arp snooping 等原因触发
IP	IP 协议栈相关模块	环路等原因触发
DHCP	DHCP 相关模块	DHCP 攻击、开启 DHCP snooping 等原因触发
TRAP	Trap 相关模块	大量告警信息触发
DT1X	802.1x 相关模块	大量 1x 用户上下线触发
SC	AAA 相关模块	大量用户认证触发
WMAC	无线终端相关模块	大量终端上下线触发
WIDS	无线 ids 防护相关模块	攻击触发
WRRM	wlan rrm 相关模块	负载均衡设置不合理等原因触发
LWPS	lwapp 隧道相关模块	大量 AP 上下线触发

```
[AC-hidecmd]display cpu-usage task
---------- Current CPU usage info ----------
CPU Usage Stat. Cycle : 27 (Second)
CPU Usage             : 6%
CPU Usage Stat. Time  : 2013-05-03  19:52:01
CPU Usage Stat. Tick  : 0xc55(CPU Tick High) 0x3fbef3eb(CPU Tick Low)
Actual Stat. Cycle    : 0x0(CPU Tick High) 0x6e987c97(CPU Tick Low)

TaskName     CPU       Runtime(CPU Tick High/CPU Tick Low)
  LPDT        0%              0/       362
  VIDL       94%              0/  68e796d7
  TICK        0%              0/    6d6aa9
  STMR        0%              0/    3ffb8f
  IPCT        0%              0/    2a8855
  DrTC        0%              0/    43b71b
  MCIN        0%              0/      6211
  IPCB        0%              0/     94150
  RPCQ        0%              0/    2563c5
  ADJ6        0%              0/      4ccf
  IPCM        0%              0/      8d7f
  INFO        0%              0/     15c59
   DEV        0%              0/    12db68
  SOCK        0%              0/     153ce
  ADJ4        0%              0/      ff9b
   ACL        0%              0/     1bd4f
  LAGG        0%              0/      c69b
  MSTP        0%              0/      d362
  PTMT        0%              0/      ac70
   ARP        0%              0/    15294c
    IP        0%              0/    2a60ba
  FSLH        0%              0/      6f2e
  FSLR        0%              0/     4e717
  NTPT        0%              0/      b0f1
  VTYD        0%              0/     8ed07
  DHCP        0%              0/     67a5c
  DHSE        0%              0/      d48f
    ND        0%              0/     75b52
  DT1X        0%              0/    305eff
   ACM        0%              0/     e0c6c
    LS        0%              0/     4e40f
  RDSO        0%              0/     2266c
   IKE        0%              0/    1b3da7
  MACA        0%              0/    1c8a76
  WAPI        0%              0/     40f9f
  PSEC        0%              0/      d81f
  STND        0%              0/     1cb0f
  ROUT        0%              0/    459b43
  WMAC        0%              0/     a3816
  WIDS        0%              0/     45890
WRRM          0%              0/     4e156
```

```
LWPS      0%      0/    744fe
IACT      0%      0/    8fc3
IFNT      0%      0/    b75f
 vt0      2%      0/    2dfdd5d
U2fT      0%      0/    283c50

[AC-hidecmd]reset task-runtime-max
[AC-hidecmd]display task
name     Tid Vid TSize Mod priority   Status        Total/Max/Last
---------------------------------------------------------------------------------
LPDT   82bfbc00  1   8  N  100        sleep        87/   0/   0
VMON   83828000  2  40  N  100   eventblock         0/   0/   0
VIDL   82bfba00  3  40  P    1 preemptready 197345147/   9/   4
TICK   82bfb800  4  40  P  250 preemptready    760264/   0/   0
STMR   82bfb600  5  40  N  150   eventblock    438369/   2/   2
IPCT   82bfb200  6  40  N  100   eventblock    298464/   0/   0
DrTC   82bfb000  7  40  N  100   eventblock    464914/   2/   2
DrTF   82c09e00  8  40  N  100   eventblock         0/   0/   0
MCIN   82c09200  9  19  N  100 preemptready      2427/   0/   0
IPCB   82c10e00 10  40  N  140   eventblock     63969/   0/   0
IPCD   82c10c00 11  40  N  100   eventblock         0/   0/   0
RPCQ   82c10a00 12  40  N  140   eventblock    261816/   0/   0
RPCD   82c10800 13  40  N  140   eventblock         0/   0/   0
  VP   82c10600 14  40  N  140   eventblock        53/   0/   0
 PAT   82c10400 15  40  N  100   eventblock         1/   0/   0
MACF   82c10200 16  40  N  100   eventblock        67/   0/   0
ADJ6   82c10000 17  40  N  100   eventblock      2120/   0/   0
MGRP   82c12e00 18  40  N  100   eventblock         1/   0/   0
IPCM   82c12c00 19  40  N  100   eventblock      3816/   0/   0
 CFM   82c12a00 20  40  N  100     queblock      4344/   0/  14
INFO   82c12800 21  40  N  100  normalready      3680/   0/   0
LGFT   82c12600 22  40  N  100   eventblock       119/   0/   0
LOAD   82c12400 23  40  N  100   eventblock         0/   0/   0
 DEV   82c12200 24  40  N  140   eventblock    129714/   2/   0
WORK   82c12000 25  40  N  100   eventblock         0/   0/   0
SOCK   82c13e00 26  40  N  100   eventblock      8617/   0/   0
ADJ4   82c13c00 27  40  N  100   eventblock      7795/   0/   0
 ACL   82c13a00 28  40  N  100   eventblock     12244/   0/   0
VLAN   82c13800 29  40  N  100   eventblock         6/   0/   0
 mac   82c13600 30  40  N  100   eventblock         0/   0/   0
LAGG   82c13400 31  40  N  140   eventblock      5453/   0/   0
MSTP   82c13200 32  40  N  100   eventblock      5693/   0/   0
PTMT   82c13000 33  40  N  100   eventblock      4733/   0/   0
PTTP   82c14e00 34  40  N  100   eventblock         0/   0/   0
 qos   82c14c00 35  40  N  100   eventblock        13/   0/   0
 ARP   82c14a00 36  40  N  100   eventblock     88993/   0/   0
  IP   82c14800 37  40  N  100   eventblock    301502/   0/   0
 NQA   82c14600 38  40  N  100   eventblock         0/   0/   0
FSLH   82c14400 39  40  N  100   eventblock      3031/   0/   0
```

```
FSLR   82c14200  40  40  N  100  eventblock   33849/   0/   0
HTTP   82c14000  41  20  N  100  eventblock       0/   0/   0
WEBS   82c15e00  42  40  N  100  eventblock       0/   0/   0
NTPT   82c15c00  43  40  N  100  eventblock    4593/   0/   0
VTYD   82c15a00  44  40  N  100  eventblock   39391/   0/   0
DHCC   82c15800  45  40  N  100  eventblock       0/   0/   0
DHCP   82c15600  46  40  N  100  eventblock   45103/   0/   0
DHSE   82c15400  47  40  N  100  eventblock    3409/   0/   0
VRRP   82c15200  48  40  N  100  eventblock       0/   0/   0
DHC6   82c15000  49  40  N  100  eventblock       0/   0/   0
DHP6   82c16e00  50  40  N  100  eventblock       0/   0/   0
DSP6   82c16c00  51  40  N  100  eventblock       0/   0/   0
FIB6   82c16a00  52  40  N  100  eventblock       1/   0/   0
FIB    82c16800  53  40  N  100  eventblock       1/   0/   0
ND     82c16600  54  40  N  100  eventblock   51868/   0/   0
AGNT   82c16400  55  40  N  100  eventblock       1/   0/   0
TRAP   82c16200  56  40  N  100  eventblock     377/   0/   0
DT1X   82c16000  57  40  N  100  eventblock  336766/   1/   1
ACM    82c17e00  58  40  N  100  eventblock   98597/   0/   0
LS     82c17c00  59  40  N  100       sleep   33116/   0/   0
RDSO   82c17a00  60  40  N  100  eventblock   16971/   0/   0
RDS    82c17800  61  40  N  100  eventblock     307/   0/   3
SC     82c17600  62  40  N  100  eventblock       0/   0/   0
TAC    82c17400  63  40  N  100  eventblock       0/   0/   0
IKE    82c17200  64  40  N  100  eventblock  196787/   0/   0
MACA   82c17000  65  40  N  100  eventblock  202843/   1/   0
NAT    82d5ce00  66  40  N  100  eventblock       0/   0/   0
PKI    82d5cc00  67  40  N  100  eventblock       7/   0/   0
PKEY   82d5ca00  68  40  N  100  eventblock       0/   0/   0
WAPI   82d5c800  69  40  N  100  eventblock   28592/   0/   0
PSEC   82d5c600  70  40  N  100  eventblock    5853/   0/   0
ALDP   82d5c400  71  40  N  100  eventblock       0/   0/   0
IGSP   82d5c200  72  40  N  100  eventblock      42/   0/   0
STND   82d5c000  73   4  N  100  eventblock   12545/   0/   0
ROUT   82d5de00  74  40  N  100  eventblock  487624/   0/   0
WMAC   82d5dc00  75  40  N  100  eventblock   68487/   0/   0
WIDS   82d5da00  76  40  N  100  eventblock   30607/   0/   0
WRRM   82d5d800  77  40  N  100  eventblock   34465/   0/   0
CWBS   82d5d600  78  40  N  100  eventblock       7/   0/   0
LWPS   82d5d400  79  40  N  100  eventblock   34705/   0/   0
IACT   82d5d200  80  40  N  100  eventblock    4022/   0/   0
IFNT   82d5d000  81  40  N  100  eventblock    5115/   0/   0
vt0    82d5ea00  82  80  N  100     running    4519/  10/   0
U2fT   82d5ec00  83  40  N  140  eventblock  284053/   0/   0
```

（3）了解当前网络是否存在重大操作

例如：

① AP 升级操作。

② 设备新上网管软件。

③ 整网重大变动。

④ 在网设备掉电、重启、异常均可能影响到无线在网设备。

⑤ 在线的一些实时操作，包括 AP 手动重启、开关服务模板等。

(4) 反馈具体操作收集信息

① 将了解到的现场操作与可以收集到的历史信息结合到一起分析，有助于判断问题。例如：

(a) AP 升级操作。

(b) 设备新上网管软件。

(c) 整网重大变动。

(d) 在网设备掉电、重启、异常均可能影响到无线在网设备。

(e) 在线的一些实时操作，包括 AP 手动重启、开关服务模板等。

② 由于当前设备恢复正常，因此只能及时收集现有的历史信息供分析。

命令：*<AC>display cpu-usage history*

　　　<AC>display diagnostic-information

进入隐藏模式。

display cpu-usage task

reset task-runtime-max

display task

例如：通过命令查看，可以确认近一个小时的 CPU 利用率具体情况。

```
<AC>display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|#####  #   ###############################
    ------------------------------------------------------------
              10        20        30        40        50        60(min)
                      cpu-usage last 60 minutes(SYSTEM)
<AC>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:
[AC-hidecmd]display cpu-usage task
```

```
---------- Current CPU usage info ----------
CPU Usage Stat. Cycle: 27 (Second)
CPU Usage             : 6%
CPU Usage Stat. Time  : 2013-05-03  19:52:01
CPU Usage Stat. Tick  : 0xc55(CPU Tick High) 0x3fbef3eb(CPU Tick Low)
Actual Stat. Cycle    : 0x0(CPU Tick High) 0x6e987c97(CPU Tick Low)

TaskName     CPU      Runtime(CPU Tick High/CPU Tick Low)
  LPDT        0%           0/      362
  VIDL       94%           0/ 68e796d7
  TICK        0%           0/   6d6aa9
  STMR        0%           0/    3ffb8f
  IPCT        0%           0/   2a8855
  DrTC        0%           0/   43b71b
  MCIN        0%           0/     6211
  IPCB        0%           0/    94150
  RPCQ        0%           0/   2563c5
  ADJ6        0%           0/     4ccf
  IPCM        0%           0/     8d7f
  INFO        0%           0/    15c59
   DEV        0%           0/   12db68
  SOCK        0%           0/    153ce
  ADJ4        0%           0/     ff9b
   ACL        0%           0/    1bd4f
  LAGG        0%           0/     c69b
  MSTP        0%           0/     d362
  PTMT        0%           0/     ac70
   ARP        0%           0/   15294c
    IP        0%           0/   2a60ba
  FSLH        0%           0/     6f2e
  FSLR        0%           0/    4e717
  NTPT        0%           0/     b0f1
  VTYD        0%           0/    8ed07
  DHCP        0%           0/    67a5c
  DHSE        0%           0/     d48f
    ND        0%           0/    75b52
  DT1X        0%           0/   305eff
   ACM        0%           0/    e0c6c
    LS        0%           0/    4e40f
  RDSO        0%           0/    2266c
   IKE        0%           0/   1b3da7
  MACA        0%           0/   1c8a76
  WAPI        0%           0/    40f9f
  PSEC        0%           0/     d81f
  STND        0%           0/    1cb0f
  ROUT        0%           0/   459b43
  WMAC        0%           0/    a3816
  WIDS        0%           0/    45890
  WRRM        0%           0/    4e156
  LWPS        0%           0/    744fe
  IACT        0%           0/     8fc3
  IFNT        0%           0/     b75f
   vt0        2%           0/  2dfdd5d
  U2fT        0%           0/   283c50
```

```
[AC-hidecmd]reset task-runtime-max
[AC-hidecmd]display task
name        Tid Vid TSize Mod priority     Status        Total/Max/Last
--------------------------------------------------------------------------------
 LPDT   82bfbc00   1    8   N   100          sleep          87/     0/    0
 VMON   83828000   2   40   N   100     eventblock           0/     0/    0
 VIDL   82bfba00   3   40   P     1   preemptready   197345147/     9/    4
 TICK   82bfb800   4   40   P   250   preemptready      760264/     0/    0
 STMR   82bfb600   5   40   N   150     eventblock      438369/     2/    2
 IPCT   82bfb200   6   40   N   100     eventblock      298464/     0/    0
 DrTC   82bfb000   7   40   N   100     eventblock      464914/     2/    2
 DrTF   82c09e00   8   40   N   100     eventblock           0/     0/    0
 MCIN   82c09200   9   19   N   100   preemptready        2427/     0/    0
 IPCB   82c10e00  10   40   N   140     eventblock       63969/     0/    0
 IPCD   82c10c00  11   40   N   100     eventblock           0/     0/    0
 RPCQ   82c10a00  12   40   N   140     eventblock      261816/     0/    0
 RPCD   82c10800  13   40   N   140     eventblock           0/     0/    0
   VP   82c10600  14   40   N   140     eventblock          53/     0/    0
  PAT   82c10400  15   40   N   100     eventblock           1/     0/    0
 MACF   82c10200  16   40   N   100     eventblock          67/     0/    0
 ADJ6   82c10000  17   40   N   100     eventblock        2120/     0/    0
 MGRP   82c12e00  18   40   N   100     eventblock           1/     0/    0
 IPCM   82c12c00  19   40   N   100     eventblock        3816/     0/    0
  CFM   82c12a00  20   40   N   100       queblock        4344/     0/   14
 INFO   82c12800  21   40   N   100    normalready        3680/     0/    0
 LGFT   82c12600  22   40   N   100     eventblock         119/     0/    0
 LOAD   82c12400  23   40   N   100     eventblock           0/     0/    0
  DEV   82c12200  24   40   N   140     eventblock      129714/     2/    0
 WORK   82c12000  25   40   N   100     eventblock           0/     0/    0
 SOCK   82c13e00  26   40   N   100     eventblock        8617/     0/    0
 ADJ4   82c13c00  27   40   N   100     eventblock        7795/     0/    0
  ACL   82c13a00  28   40   N   100     eventblock       12244/     0/    0
 VLAN   82c13800  29   40   N   100     eventblock           6/     0/    0
  mac   82c13600  30   40   N   100     eventblock           0/     0/    0
 LAGG   82c13400  31   40   N   140     eventblock        5453/     0/    0
 MSTP   82c13200  32   40   N   100     eventblock        5693/     0/    0
 PTMT   82c13000  33   40   N   100     eventblock        4733/     0/    0
 PTTP   82c14e00  34   40   N   100     eventblock           0/     0/    0
  qos   82c14c00  35   40   N   100     eventblock          13/     0/    0
  ARP   82c14a00  36   40   N   100     eventblock       88993/     0/    0
   IP   82c14800  37   40   N   100     eventblock      301502/     0/    0
  NQA   82c14600  38   40   N   100     eventblock           0/     0/    0
 FSLH   82c14400  39   40   N   100     eventblock        3031/     0/    0
 FSLR   82c14200  40   40   N   100     eventblock       33849/     0/    0
 HTTP   82c14000  41   20   N   100     eventblock           0/     0/    0
 WEBS   82c15e00  42   40   N   100     eventblock           0/     0/    0
 NTPT   82c15c00  43   40   N   100     eventblock        4593/     0/    0
 VTYD   82c15a00  44   40   N   100     eventblock       39391/     0/    0
 DHCC   82c15800  45   40   N   100     eventblock           0/     0/    0
 DHCP   82c15600  46   40   N   100     eventblock       45103/     0/    0
 DHSE   82c15400  47   40   N   100     eventblock        3409/     0/    0
```

VRRP	82c15200	48	40	N	100	eventblock	0/	0/	0
DHC6	82c15000	49	40	N	100	eventblock	0/	0/	0
DHP6	82c16e00	50	40	N	100	eventblock	0/	0/	0
DSP6	82c16c00	51	40	N	100	eventblock	0/	0/	0
FIB6	82c16a00	52	40	N	100	eventblock	1/	0/	0
FIB	82c16800	53	40	N	100	eventblock	1/	0/	0
ND	82c16600	54	40	N	100	eventblock	51868/	0/	0
AGNT	82c16400	55	40	N	100	eventblock	1/	0/	0
TRAP	82c16200	56	40	N	100	eventblock	377/	0/	0
DT1X	82c16000	57	40	N	100	eventblock	336766/	1/	1
ACM	82c17e00	58	40	N	100	eventblock	98597/	0/	0
LS	82c17c00	59	40	N	100	sleep	33116/	0/	0
RDSO	82c17a00	60	40	N	100	eventblock	16971/	0/	0
RDS	82c17800	61	40	N	100	eventblock	307/	0/	3
SC	82c17600	62	40	N	100	eventblock	0/	0/	0
TAC	82c17400	63	40	N	100	eventblock	0/	0/	0
IKE	82c17200	64	40	N	100	eventblock	196787/	0/	0
MACA	82c17000	65	40	N	100	eventblock	202843/	1/	0
NAT	82d5ce00	66	40	N	100	eventblock	0/	0/	0
PKI	82d5cc00	67	40	N	100	eventblock	7/	0/	0
PKEY	82d5ca00	68	40	N	100	eventblock	0/	0/	0
WAPI	82d5c800	69	40	N	100	eventblock	28592/	0/	0
PSEC	82d5c600	70	40	N	100	eventblock	5853/	0/	0
ALDP	82d5c400	71	40	N	100	eventblock	0/	0/	0
IGSP	82d5c200	72	40	N	100	eventblock	42/	0/	0
STND	82d5c000	73	4	N	100	eventblock	12545/	0/	0
ROUT	82d5de00	74	40	N	100	eventblock	487624/	0/	0
WMAC	82d5dc00	75	40	N	100	eventblock	68487/	0/	0
WIDS	82d5da00	76	40	N	100	eventblock	30607/	0/	0
WRRM	82d5d800	77	40	N	100	eventblock	34465/	0/	0
CWBS	82d5d600	78	40	N	100	eventblock	7/	0/	0
LWPS	82d5d400	79	40	N	100	eventblock	34705/	0/	0
IACT	82d5d200	80	40	N	100	eventblock	4022/	0/	0
IFNT	82d5d000	81	40	N	100	eventblock	5115/	0/	0
vt0	82d5ea00	82	80	N	100	running	4519/	10/	0
U2fT	82d5ec00	83	40	N	140	eventblock	284053/	0/	0

（5）收集信息

命令：<AC>*display cpu-usage history*

<AC>*display diagnostic-information*

进入隐藏模式。

display cpu-usage task

reset task-runtime-max

display task

例如：通过命令查看，可以确认近一个小时的 CPU 利用率具体情况。

```
<AC>display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|##### #   ###############################
     ------------------------------------------------------------
              10        20        30        40        50        60(min)
                      cpu-usage last 60 minutes(SYSTEM)
<AC>display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:

[AC-hidecmd]display cpu-usage task
---------- Current CPU usage info ----------
CPU Usage Stat. Cycle : 27 (Second)
CPU Usage             : 6%
CPU Usage Stat. Time  : 2013-05-03  19:52:01
CPU Usage Stat. Tick  : 0xc55(CPU Tick High) 0x3fbef3eb(CPU Tick Low)
Actual Stat. Cycle    : 0x0(CPU Tick High) 0x6e987c97(CPU Tick Low)

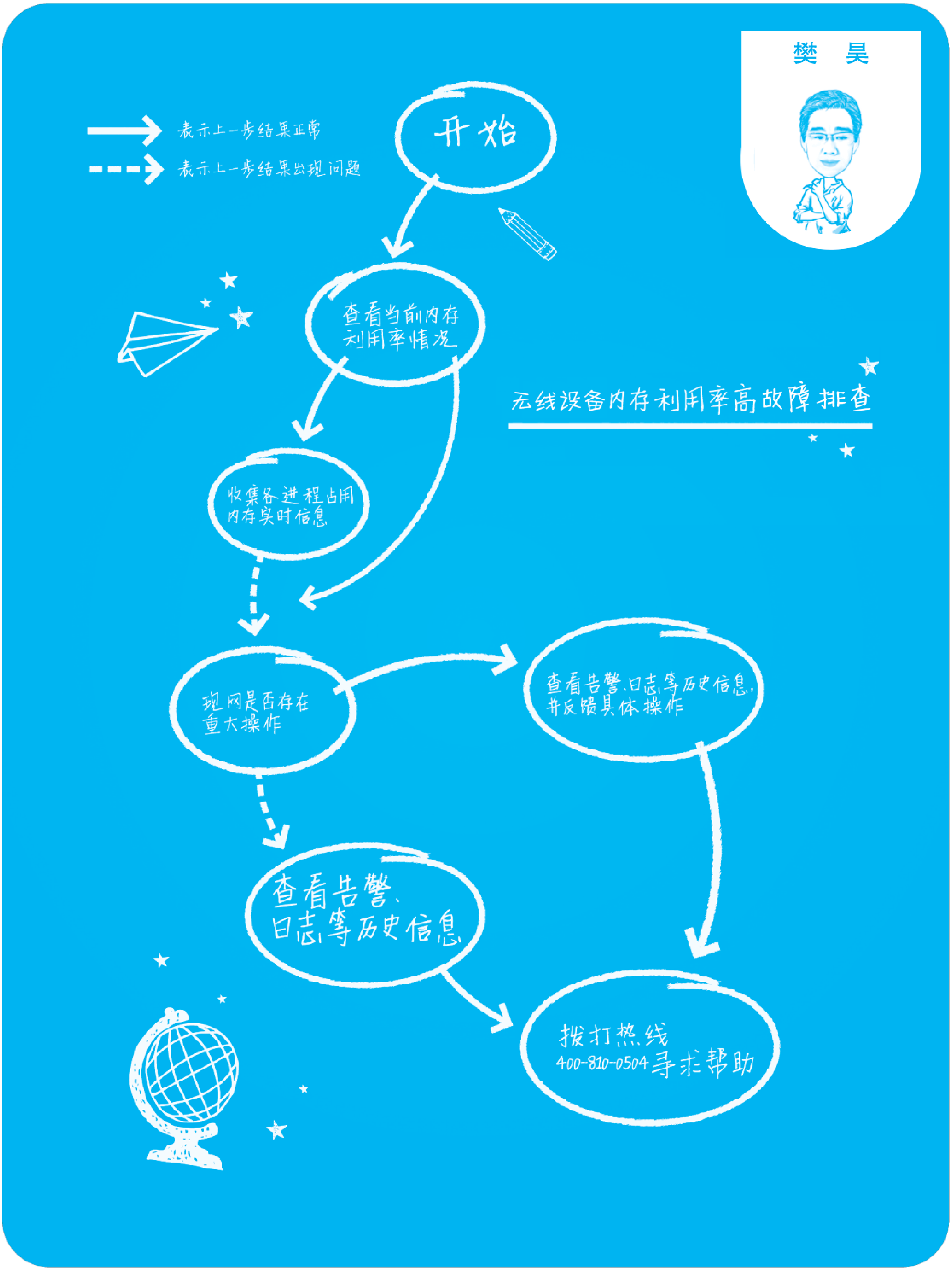
TaskName        CPU       Runtime(CPU Tick High/CPU Tick Low)
 LPDT           0%               0/       362
 VIDL          94%               0/  68e796d7
 TICK           0%               0/    6d6aa9
 STMR           0%               0/    3ffb8f
 IPCT           0%               0/    2a8855
 DrTC           0%               0/    43b71b
 MCIN           0%               0/      6211
 IPCB           0%               0/     94150
 RPCQ           0%               0/    2563c5
 ADJ6           0%               0/      4ccf
 IPCM           0%               0/      8d7f
 INFO           0%               0/     15c59
 DEV            0%               0/    12db68
 SOCK           0%               0/     153ce
```

```
     ADJ4          0%            0/        ff9b
      ACL          0%            0/       1bd4f
     LAGG          0%            0/        c69b
     MSTP          0%            0/        d362
     PTMT          0%            0/        ac70
      ARP          0%            0/      15294c
       IP          0%            0/      2a60ba
     FSLH          0%            0/        6f2e
     FSLR          0%            0/       4e717
     NTPT          0%            0/        b0f1
     VTYD          0%            0/       8ed07
     DHCP          0%            0/       67a5c
     DHSE          0%            0/        d48f
       ND          0%            0/       75b52
     DT1X          0%            0/      305eff
      ACM          0%            0/       e0c6c
       LS          0%            0/       4e40f
     RDSO          0%            0/       2266c
      IKE          0%            0/      1b3da7
     MACA          0%            0/      1c8a76
     WAPI          0%            0/       40f9f
     PSEC          0%            0/        d81f
     STND          0%            0/       1cb0f
     ROUT          0%            0/      459b43
     WMAC          0%            0/       a3816
     WIDS          0%            0/       45890
     WRRM          0%            0/       4e156
     LWPS          0%            0/       744fe
     IACT          0%            0/        8fc3
     IFNT          0%            0/        b75f
      vt0          2%            0/     2dfdd5d
     U2fT          0%            0/      283c50

[AC-hidecmd]reset task-runtime-max
[AC-hidecmd]display task
name   Tid Vid TSize Mod priority    Status   Total/Max/Last
---------------------------------------------------------------------------
  LPDT   82bfbc00   1    8   N   100          sleep         87/    0/    0
  VMON   83828000   2   40   N   100     eventblock          0/    0/    0
  VIDL   82bfba00   3   40   P     1   preemptready  197345147/    9/    4
  TICK   82bfb800   4   40   P   250   preemptready     760264/    0/    0
  STMR   82bfb600   5   40   N   150     eventblock     438369/    2/    2
  IPCT   82bfb200   6   40   N   100     eventblock     298464/    0/    0
  DrTC   82bfb000   7   40   N   100     eventblock     464914/    2/    2
  DrTF   82c09e00   8   40   N   100     eventblock          0/    0/    0
  MCIN   82c09200   9   19   N   100   preemptready       2427/    0/    0
  IPCB   82c10e00  10   40   N   140     eventblock      63969/    0/    0
  IPCD   82c10c00  11   40   N   100     eventblock          0/    0/    0
  RPCQ   82c10a00  12   40   N   140     eventblock     261816/    0/    0
```

```
      RPCD   82c10800  13  40  N  140      eventblock        0/    0/    0
        VP   82c10600  14  40  N  140      eventblock       53/    0/    0
       PAT   82c10400  15  40  N  100      eventblock        1/    0/    0
      MACF   82c10200  16  40  N  100      eventblock       67/    0/    0
      ADJ6   82c10000  17  40  N  100      eventblock     2120/    0/    0
      MGRP   82c12e00  18  40  N  100      eventblock        1/    0/    0
      IPCM   82c12c00  19  40  N  100      eventblock     3816/    0/    0
       CFM   82c12a00  20  40  N  100        queblock     4344/    0/   14
      INFO   82c12800  21  40  N  100     normalready     3680/    0/    0
      LGFT   82c12600  22  40  N  100      eventblock      119/    0/    0
      LOAD   82c12400  23  40  N  100      eventblock        0/    0/    0
       DEV   82c12200  24  40  N  140      eventblock   129714/    2/    0
      WORK   82c12000  25  40  N  100      eventblock        0/    0/    0
      SOCK   82c13e00  26  40  N  100      eventblock     8617/    0/    0
      ADJ4   82c13c00  27  40  N  100      eventblock     7795/    0/    0
       ACL   82c13a00  28  40  N  100      eventblock    12244/    0/    0
      VLAN   82c13800  29  40  N  100      eventblock        6/    0/    0
       mac   82c13600  30  40  N  100      eventblock        0/    0/    0
      LAGG   82c13400  31  40  N  140      eventblock     5453/    0/    0
      MSTP   82c13200  32  40  N  100      eventblock     5693/    0/    0
      PTMT   82c13000  33  40  N  100      eventblock     4733/    0/    0
      PTTP   82c14e00  34  40  N  100      eventblock        0/    0/    0
       qos   82c14c00  35  40  N  100      eventblock       13/    0/    0
       ARP   82c14a00  36  40  N  100      eventblock    88993/    0/    0
        IP   82c14800  37  40  N  100      eventblock   301502/    0/    0
       NQA   82c14600  38  40  N  100      eventblock        0/    0/    0
      FSLH   82c14400  39  40  N  100      eventblock     3031/    0/    0
      FSLR   82c14200  40  40  N  100      eventblock    33849/    0/    0
      HTTP   82c14000  41  20  N  100      eventblock        0/    0/    0
      WEBS   82c15e00  42  40  N  100      eventblock        0/    0/    0
      NTPT   82c15c00  43  40  N  100      eventblock     4593/    0/    0
      VTYD   82c15a00  44  40  N  100      eventblock    39391/    0/    0
      DHCC   82c15800  45  40  N  100      eventblock        0/    0/    0
      DHCP   82c15600  46  40  N  100      eventblock    45103/    0/    0
      DHSE   82c15400  47  40  N  100      eventblock     3409/    0/    0
      VRRP   82c15200  48  40  N  100      eventblock        0/    0/    0
      DHC6   82c15000  49  40  N  100      eventblock        0/    0/    0
      DHP6   82c16e00  50  40  N  100      eventblock        0/    0/    0
      DSP6   82c16c00  51  40  N  100      eventblock        0/    0/    0
      FIB6   82c16a00  52  40  N  100      eventblock        1/    0/    0
       FIB   82c16800  53  40  N  100      eventblock        1/    0/    0
        ND   82c16600  54  40  N  100      eventblock    51868/    0/    0
      AGNT   82c16400  55  40  N  100      eventblock        1/    0/    0
      TRAP   82c16200  56  40  N  100      eventblock      377/    0/    0
      DT1X   82c16000  57  40  N  100      eventblock   336766/    1/    1
       ACM   82c17e00  58  40  N  100      eventblock    98597/    0/    0
        LS   82c17c00  59  40  N  100           sleep    33116/    0/    0
      RDSO   82c17a00  60  40  N  100      eventblock    16971/    0/    0
       RDS   82c17800  61  40  N  100      eventblock      307/    0/    3
        SC   82c17600  62  40  N  100      eventblock        0/    0/    0
```

```
TAC   82c17400  63  40  N  100  eventblock      0/   0/  0
IKE   82c17200  64  40  N  100  eventblock 196787/   0/  0
MACA  82c17000  65  40  N  100  eventblock 202843/   1/  0
NAT   82d5ce00  66  40  N  100  eventblock      0/   0/  0
PKI   82d5cc00  67  40  N  100  eventblock      7/   0/  0
PKEY  82d5ca00  68  40  N  100  eventblock      0/   0/  0
WAPI  82d5c800  69  40  N  100  eventblock  28592/   0/  0
PSEC  82d5c600  70  40  N  100  eventblock   5853/   0/  0
ALDP  82d5c400  71  40  N  100  eventblock      0/   0/  0
IGSP  82d5c200  72  40  N  100  eventblock     42/   0/  0
STND  82d5c000  73   4  N  100  eventblock  12545/   0/  0
ROUT  82d5de00  74  40  N  100  eventblock 487624/   0/  0
WMAC  82d5dc00  75  40  N  100  eventblock  68487/   0/  0
WIDS  82d5da00  76  40  N  100  eventblock  30607/   0/  0
WRRM  82d5d800  77  40  N  100  eventblock  34465/   0/  0
CWBS  82d5d600  78  40  N  100  eventblock      7/   0/  0
LWPS  82d5d400  79  40  N  100  eventblock  34705/   0/  0
IACT  82d5d200  80  40  N  100  eventblock   4022/   0/  0
IFNT  82d5d000  81  40  N  100  eventblock   5115/   0/  0
vt0   82d5ea00  82  80  N  100     running   4519/  10/  0
U2fT  82d5ec00  83  40  N  140  eventblock 284053/   0/  0
```


樊 昊
表示上一步结果正常
表示上一步结果出现问题
开始
查看当前内存利用率情况
无线设备内存利用率高故障排查
收集各进程占用内存实时信息
现网是否存在重大操作
查看告警、日志等历史信息，并反馈具体操作
查看告警、日志等历史信息
拨打热线 400-810-0504寻求帮助

1. 开始

内存利用率异常问题，属于比较罕见的现象，但是一旦问题发生就是非常危险的情况，需要及时收集信息，分析问题原因，将问题的影响度降到最低。

定位故障的思路如下。

① 判断当前内存是否正常。

② 判断近期操作是否影响到内存。

③ 判断具体是哪个进程长时间占用内存。

2. 流程图相关操作说明

（1）查看当前内存利用率情况

通过及时查看当前内存利用率实时状态，可以判断问题的严重程度，也能第一时间收集更多的有用信息，以便明确下一步操作。

命令：*display cpu-usage*

例如：通过命令查看，可以确认当前内存是正常状态（高于70%且出现持续增长则表示异常）。

```
[AC]display memory
System Total Memory(bytes): 533578560
Total Used Memory(bytes): 111957472
Used Rate: 20%
```

（2）收集各进程占用内存实时信息

命令：*[AC-hidecmd]_display memory 32 group core 0*

[AC-hidecmd]_display memory 64 core 0

[AC-hidecmd]_display memory 128 group core 0

[AC-hidecmd]_display memory 256 group core 0

[AC-hidecmd]_display memory 512 group core 0

[AC-hidecmd]_display memory 1024 group core 0

[AC-hidecmd]_display memory 2048 group core 0

[AC-hidecmd]_display memory 4096 group core 0

```
[AC-hidecmd]_display memory 32 group core 0
(0106,       216) (010d,         6) (0801,         6) (0802,         5)
(0b00,         1) (0270,        14) (0341,       539) (0110,        51)
(0805,         8) (0822,         1) (0804,         2) (0831,       161)
(0830,       140) (0213,      1250) (0828,        26) (0833,         5)
(0806,         3) (0826,         7) (0214,      1806) (0215,       199)
(0216,      4469) (042e,        24) (021e,         2) (0240,       116)
(0900,       813) (0468,         2) (0c43,        65) (0230,       168)
(0d20,       188) (0311,         8) (0310,         5) (0360,         1)
(041e,        33) (0518,         2) (0846,        23) (0b28,        34)
```

```
(0b02,     34) (0b0e,      9) (0d10,     67) (0505,      8)
(0543,      2) (0125,     10) (04d2,      1) (010c,     10)
(0276,      1) (0b23,      8) (0274,      1) (0292,      8)
(0b01,     27) (043a,      9) (0277,      4) (0501,     43)
(0279,      1) (0260,      4) (cc16,     10) (0263,      4)
(0446,     23) (04c9,     21) (0467,      4) (040c,     11)
(0401,      4) (0418,      2) (042a,      1) (0c62,      1)
(04c4,      6) (0c21,      6) (0c23,     16) (04ca,     16)
(0342,     14) (0816,      4) (0320,     46) (0321,      6)
(0817,      3) (0387,      2) (0c71,     70) (0c83,     27)
(0490,     16) (0526,     12) (0528,     11) (0c22,     16)
(04a0,     17) (0504,      1) (0502,      1) (0491,      1)
(0509,      4) (0537,     10) (0515,      1) (0553,      2)
(0428,      1) (0340,      7) (02b5,      1) (0524,      2)
(0523,      5) (0c12,      4) (0425,      4) (0904,      2)
(0538,     12) (0b11,      1) (0c3b,      3) (0527,      5)
(0810,      2) (0498,     12) (0c26,     12) (0b0c,      3)
(0217,    202) (0602,      7) (04cb,      4) (0b18,     12)
(0b22,      5) (0cd4,      1) (0514,      9) (0811,      6)
(034c,      6) (0c36,      3) (0911,     94) (0516,     10)
(0c60,      2) (085a,      4) (0532,      1) (0cb6,      2)
(0807,      1) (0813,      5) (0cb8,      1) (0000,      0)
```

```
[AC-hidecmd]_display memory 64 core 0
Block Size    64        Free     7       Used   3820       Total   3827
-------------------------Block From     0-------------------------
(d0333b40, 02600000)  (d0333ba0, 02600000)  (d0333c00, 02600000)
(d0333c60, 011e0025)  (d0333cc0, 01101001)  (d0333d20, 01101001)
(d0333d80, 011e0025)  (d0333de0, 011e0025)  (d0333e40, 01106002)
(d0333ea0, 01109001)  (d0333f00, 01109001)
```

```
[AC-hidecmd]_display memory 128 group core 0
(cc00,      1) (cc03,      1) (0846,      2) (0801,     17)
(0802,     17) (0276,      1) (0110,     37) (0830,      2)
(0806,     22) (0214,    480) (0216,    500) (0b28,      1)
(0c43,      9) (0240,    106) (0d20,    452) (0b25,      1)
(0833,      1) (0310,      1) (0213,     34) (0218,      3)
(0278,      1) (0260,      1) (0490,      3) (0501,      4)
(0c71,     24) (0101,      2) (04a0,     12) (0102,      1)
(0125,      2) (0cb9,      3) (0cb6,      1) (0b0b,      2)
(011c,      2) (0ca0,     23) (0c11,     23) (0230,     19)
(0340,      2) (04c4,      2) (0468,      2) (0525,      2)
(0c14,      2) (0816,      2) (0b23,      2) (0b0c,      6)
(0b02,      1) (0900,      4) (0b01,      3) (0538,     10)
(041e,      8) (0527,      5) (0c2a,      7) (0000,      0)
```

```
[AC-hidecmd]_display memory 256 group core 0
(02f0,          1) (011c,         27) (0110,          2) (021b,          1)
(0830,          1) (0806,          2) (0213,        214) (0283,          1)
(0214,        850) (0125,        130) (040c,          1) (0b0c,          2)
(0101,         11) (04d2,         16) (0216,         78) (0c01,          1)
(010c,          1) (0c00,          2) (0240,         55) (042a,          1)
(0102,          3) (0c43,          2) (0425,          1) (0341,        501)
(0342,         91) (0523,          1) (0810,          1) (0320,         29)
(0c72,         13) (0c71,         21) (0420,          1) (0502,          1)
(0504,          1) (0491,          1) (0483,          1) (04a0,          7)
(043a,          1) (042e,          7) (0813,          1) (0869,          2)
(0807,          1) (0600,          1) (0661,          1) (0b05,        181)
(0b0b,          2) (0446,         23) (cc15,          2) (cc16,          5)
(041e,         16) (0467,          2) (0428,          2) (0c30,          6)
(0816,          1) (0b18,          1) (0846,          1) (0526,          5)
(0b01,          4) (0b02,          9) (0b11,          2) (0b23,          1)
(0b0d,          1) (0514,          1) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 512 group core 0
(0117,          1) (cc00,          1) (011e,          4) (0110,          7)
(0cb6,          1) (0813,          1) (0c43,         13) (0c00,          1)
(0c01,          1) (0341,          1) (0216,         28) (0360,          1)
(041e,          2) (04ca,          1) (04c9,          1) (0532,          1)
(0125,         10) (04d2,          1) (051d,          4) (0260,          2)
(0213,          3) (0230,          9) (040c,          1) (0342,         11)
(0c72,          3) (0240,         10) (0c0e,          1) (04a0,         23)
(04a6,          2) (0102,          3) (0869,          2) (0602,          1)
(0101,          1) (0b1a,          1) (0801,         16) (0501,          4)
(085a,         11) (0526,         10) (0b02,          5) (0278,          3)
(0d20,         68) (0b01,          2) (0214,        205) (0217,         20)
(0c2b,          1) (0000,          0) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 1024 group core 0
(0118,          1) (010d,          1) (0160,          5) (0110,         38)
(021b,          1) (085f,          1) (0216,        108) (0c71,          1)
(021c,          4) (0215,       1004) (0cb8,          1) (0101,          3)
(0602,          2) (011e,          1) (0cb6,          1) (0900,          1)
(041e,          1) (051c,          1) (0508,          1) (0b28,          4)
(0b01,          1) (0d10,          1) (0509,          8) (04d2,          2)
(0518,         10) (0b0b,          1) (cc16,         10) (0320,          5)
(0b11,          1) (cc15,          2) (04a0,          4) (0102,          4)
(011c,          1) (0490,          3) (0214,          3) (0264,          1)
(0260,          1) (0b13,          1) (0b18,          2) (0213,          1)
(0b05,         68) (040c,          1) (0b02,         14) (0d20,          1)
(0217,        139) (0278,          2) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 2048 group core 0
(0118,          1) (0101,          10) (0102,          46) (0110,           2)
(010f,          2) (0821,           5) (021b,           1) (0283,          14)
(0111,          1) (0d10,           1) (0125,           8) (0218,          10)
(0260,          1) (0216,          10) (0264,           1) (042a,           1)
(0341,          3) (040c,           1) (0342,           5) (0425,           1)
(0cc5,          1) (0661,           2) (0420,           5) (0502,           1)
(0504,          1) (0491,           1) (04a0,          16) (cc16,           5)
(043a,          1) (0523,           1) (042e,           1) (0805,           5)
(0813,          1) (0807,           1) (0cb6,           1) (0602,           6)
(0000,          2) (0600,           7) (ccc8,           1) (0810,           2)
(011c,          1) (0525,           2) (011e,           1) (0526,           2)
(0217,          1) (0278,           1) (0000,           0) (0000,           0)
```

```
[AC-hidecmd]_display memory 4096 group core 0
(0160,          1) (010f,           1) (0110,           1) (0822,           1)
(0813,          2) (0821,           1) (01ff,        1381) (0111,         200)
(0c43,         18) (0102,           8) (0b02,           4) (0101,           9)
(0b28,          1) (0b01,           1) (0911,           1) (0216,          13)
(0c44,          1) (0230,           2) (0342,           1) (0321,           4)
(0501,          1) (0517,           2) (011e,           2) (0537,           1)
(0516,          1) (04a0,          10) (0805,           5) (011c,           1)
(0602,          9) (0c60,           2) (0b0b,           1) (0b13,           1)
(0240,          2) (ccc8,           1) (0509,           2) (0816,           1)
(0c28,          3) (0514,           1) (0000,           0) (0000,           0)
```

(3) 现网是否存在重大操作

① 例如新增网管，对设备开始采集信息。

② 增加新配置，新功能，如 IPSec、ARP Snooping 功能等。

(4) 查看告警、日志等历史信息并反馈具体操作

① 命令：*<AC>display trapbuffer*

<AC>display logbuffer

[AC-hidecmd]_display memory 32 group core 0

[AC-hidecmd]_display memory 64 core 0

[AC-hidecmd]_display memory 128 group core 0

[AC-hidecmd]_display memory 256 group core 0

[AC-hidecmd]_display memory 512 group core 0

[AC-hidecmd]_display memory 1024 group core 0

[AC-hidecmd]_display memory 2048 group core 0

[AC-hidecmd]_display memory 4096 group core 0

```
[AC-hidecmd]_display memory 32 group core 0
(0106,        216) (010d,           6) (0801,           6) (0802,           5)
(0b00,          1) (0270,          14) (0341,         539) (0110,          51)
(0805,          8) (0822,           1) (0804,           2) (0831,         161)
```

```
(0830,       140) (0213,      1250) (0828,        26) (0833,         5)
(0806,         3) (0826,         7) (0214,      1806) (0215,       199)
(0216,      4469) (042e,        24) (021e,         2) (0240,       116)
(0900,       813) (0468,         2) (0c43,        65) (0230,       168)
(0d20,       188) (0311,         8) (0310,         5) (0360,         1)
(041e,        33) (0518,         2) (0846,        23) (0b28,        34)
(0b02,        34) (0b0e,         9) (0d10,        67) (0505,         8)
(0543,         2) (0125,        10) (04d2,         1) (010c,        10)
(0276,         1) (0b23,         8) (0274,         1) (0292,         8)
(0b01,        27) (043a,         9) (0277,         4) (0501,        43)
(0279,         1) (0260,         4) (cc16,        10) (0263,         4)
(0446,        23) (04c9,        21) (0467,         4) (040c,        11)
(0401,         4) (0418,         2) (042a,         1) (0c62,         1)
(04c4,         6) (0c21,         6) (0c23,        16) (04ca,        16)
(0342,        14) (0816,         4) (0320,        46) (0321,         6)
(0817,         3) (0387,         2) (0c71,        70) (0c83,        27)
(0490,        16) (0526,        12) (0528,        11) (0c22,        16)
(04a0,        17) (0504,         1) (0502,         1) (0491,         1)
(0509,         4) (0537,        10) (0515,         1) (0553,         2)
(0428,         1) (0340,         7) (02b5,         1) (0524,         2)
(0523,         5) (0c12,         4) (0425,         4) (0904,         2)
(0538,        12) (0b11,         1) (0c3b,         3) (0527,         5)
(0810,         2) (0498,        12) (0c26,        12) (0b0c,         3)
(0217,       202) (0602,         7) (04cb,         4) (0b18,        12)
(0b22,         5) (0cd4,         1) (0514,         9) (0811,         6)
(034c,         6) (0c36,         3) (0911,        94) (0516,        10)
(0c60,         2) (085a,         4) (0532,         1) (0cb6,         2)
(0807,         1) (0813,         5) (0cb8,         1) (0000,         0)
```

```
[AC-hidecmd]_display memory 64 core 0
Block Size    64        Free    7       Used   3820      Total   3827
-------------------------Block From     0-------------------------
(d0333b40, 02600000)  (d0333ba0, 02600000)  (d0333c00, 02600000)
(d0333c60, 011e0025)  (d0333cc0, 01101001)  (d0333d20, 01101001)
(d0333d80, 011e0025)  (d0333de0, 011e0025)  (d0333e40, 01106002)
(d0333ea0, 01109001)  (d0333f00, 01109001)
```

```
[AC-hidecmd]_display memory 128 group core 0
(cc00,         1) (cc03,         1) (0846,         2) (0801,        17)
(0802,        17) (0276,         1) (0110,        37) (0830,         2)
(0806,        22) (0214,       480) (0216,       500) (0b28,         1)
(0c43,         9) (0240,       106) (0d20,       452) (0b25,         1)
(0833,         1) (0310,         1) (0213,        34) (0218,         3)
(0278,         1) (0260,         1) (0490,         3) (0501,         4)
(0c71,        24) (0101,         2) (04a0,        12) (0102,         1)
(0125,         2) (0cb9,         3) (0cb6,         1) (0b0b,         2)
(011c,         2) (0ca0,        23) (0c11,        23) (0230,        19)
(0340,         2) (04c4,         2) (0468,         2) (0525,         2)
(0c14,         2) (0816,         2) (0b23,         2) (0b0c,         6)
(0b02,         1) (0900,         4) (0b01,         3) (0538,        10)
(041e,         8) (0527,         5) (0c2a,         7) (0000,         0)
```

```
[AC-hidecmd]_display memory 256 group core 0
(02f0,          1) (011c,         27) (0110,          2) (021b,          1)
(0830,          1) (0806,          2) (0213,        214) (0283,          1)
(0214,        850) (0125,        130) (040c,          1) (0b0c,          2)
(0101,         11) (04d2,         16) (0216,         78) (0c01,          1)
(010c,          1) (0c00,          2) (0240,         55) (042a,          1)
(0102,          3) (0c43,          2) (0425,          1) (0341,        501)
(0342,         91) (0523,          1) (0810,          1) (0320,         29)
(0c72,         13) (0c71,         21) (0420,          1) (0502,          1)
(0504,          1) (0491,          1) (0483,          1) (04a0,          7)
(043a,          1) (042e,          7) (0813,          1) (0869,          2)
(0807,          1) (0600,          1) (0661,          1) (0b05,        181)
(0b0b,          2) (0446,         23) (cc15,          2) (cc16,          5)
(041e,         16) (0467,          2) (0428,          2) (0c30,          6)
(0816,          1) (0b18,          1) (0846,          1) (0526,          5)
(0b01,          4) (0b02,          9) (0b11,          2) (0b23,          1)
(0b0d,          1) (0514,          1) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 512 group core 0
(0117,          1) (cc00,          1) (011e,          4) (0110,          7)
(0cb6,          1) (0813,          1) (0c43,         13) (0c00,          1)
(0c01,          1) (0341,          1) (0216,         28) (0360,          1)
(041e,          2) (04ca,          1) (04c9,          1) (0532,          1)
(0125,         10) (04d2,          1) (051d,          4) (0260,          2)
(0213,          3) (0230,          9) (040c,          1) (0342,         11)
(0c72,          3) (0240,         10) (0c0e,          1) (04a0,         23)
(04a6,          2) (0102,          3) (0869,          2) (0602,          1)
(0101,          1) (0b1a,          1) (0801,         16) (0501,          4)
(085a,         11) (0526,         10) (0b02,          5) (0278,          3)
(0d20,         68) (0b01,          2) (0214,        205) (0217,         20)
(0c2b,          1) (0000,          0) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 1024 group core 0
(0118,          1) (010d,          1) (0160,          5) (0110,         38)
(021b,          1) (085f,          1) (0216,        108) (0c71,          1)
(021c,          4) (0215,       1004) (0cb8,          1) (0101,          3)
(0602,          2) (011e,          1) (0cb6,          1) (0900,          1)
(041e,          1) (051c,          1) (0508,          1) (0b28,          4)
(0b01,          1) (0d10,          1) (0509,          8) (04d2,          2)
(0518,         10) (0b0b,          1) (cc16,         10) (0320,          5)
(0b11,          1) (cc15,          2) (04a0,          4) (0102,          4)
(011c,          1) (0490,          3) (0214,          3) (0264,          1)
(0260,          1) (0b13,          1) (0b18,          2) (0213,          1)
(0b05,         68) (040c,          1) (0b02,         14) (0d20,          1)
(0217,        139) (0278,          2) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 2048 group core 0
(0118,         1) (0101,        10) (0102,        46) (0110,         2)
(010f,         2) (0821,         5) (021b,         1) (0283,        14)
(0111,         1) (0d10,         1) (0125,         8) (0218,        10)
(0260,         1) (0216,        10) (0264,         1) (042a,         1)
(0341,         3) (040c,         1) (0342,         5) (0425,         1)
(0cc5,         1) (0661,         2) (0420,         5) (0502,         1)
(0504,         1) (0491,         1) (04a0,        16) (cc16,         5)
(043a,         1) (0523,         1) (042e,         1) (0805,         5)
(0813,         1) (0807,         1) (0cb6,         1) (0602,         6)
(0000,         2) (0600,         7) (ccc8,         1) (0810,         2)
(011c,         1) (0525,         2) (011e,         1) (0526,         2)
(0217,         1) (0278,         1) (0000,         0) (0000,         0)
```

```
[AC-hidecmd]_display memory 4096 group core 0
(0160,         1) (010f,         1) (0110,         1) (0822,         1)
(0813,         2) (0821,         1) (01ff,      1381) (0111,       200)
(0c43,        18) (0102,         8) (0b02,         4) (0101,         9)
(0b28,         1) (0b01,         1) (0911,         1) (0216,        13)
(0c44,         1) (0230,         2) (0342,         1) (0321,         4)
(0501,         1) (0517,         2) (011e,         2) (0537,         1)
(0516,         1) (04a0,        10) (0805,         5) (011c,         1)
(0602,         9) (0c60,         2) (0b0b,         1) (0b13,         1)
(0240,         2) (ccc8,         1) (0509,         2) (0816,         1)
(0c28,         3) (0514,         1) (0000,         0) (0000,         0)
```

② 反馈信息举例。例如，当多网管对设备同时采集信息时，可能会导致内存泄漏，此时可以关闭新上的网管观察效果。

(5) 查看告警、日志等历史信息

<AC>display trapbuffer

<AC>display logbuffer

[AC-hidecmd]_display memory 32 group core 0

[AC-hidecmd]_display memory 64 core 0

[AC-hidecmd]_display memory 128 group core 0

[AC-hidecmd]_display memory 256 group core 0

[AC-hidecmd]_display memory 512 group core 0

[AC-hidecmd]_display memory 1024 group core 0

[AC-hidecmd]_display memory 2048 group core 0

[AC-hidecmd]_display memory 4096 group core 0

```
[AC-hidecmd]_display memory 32 group core 0
(0106,       216) (010d,         6) (0801,         6) (0802,         5)
(0b00,         1) (0270,        14) (0341,       539) (0110,        51)
(0805,         8) (0822,         1) (0804,         2) (0831,       161)
(0830,       140) (0213,      1250) (0828,        26) (0833,         5)
```

```
(0806,      3) (0826,      7) (0214,   1806) (0215,    199)
(0216,   4469) (042e,     24) (021e,      2) (0240,    116)
(0900,    813) (0468,      2) (0c43,     65) (0230,    168)
(0d20,    188) (0311,      8) (0310,      5) (0360,      1)
(041e,     33) (0518,      2) (0846,     23) (0b28,     34)
(0b02,     34) (0b0e,      9) (0d10,     67) (0505,      8)
(0543,      2) (0125,     10) (04d2,      1) (010c,     10)
(0276,      1) (0b23,      8) (0274,      1) (0292,      8)
(0b01,     27) (043a,      9) (0277,      4) (0501,     43)
(0279,      1) (0260,      4) (cc16,     10) (0263,      4)
(0446,     23) (04c9,     21) (0467,      4) (040c,     11)
(0401,      4) (0418,      2) (042a,      1) (0c62,      1)
(04c4,      6) (0c21,      6) (0c23,     16) (04ca,     16)
(0342,     14) (0816,      4) (0320,     46) (0321,      6)
(0817,      3) (0387,      2) (0c71,     70) (0c83,     27)
(0490,     16) (0526,     12) (0528,     11) (0c22,     16)
(04a0,     17) (0504,      1) (0502,      1) (0491,      1)
(0509,      4) (0537,     10) (0515,      1) (0553,      2)
(0428,      1) (0340,      7) (02b5,      1) (0524,      2)
(0523,      5) (0c12,      4) (0425,      4) (0904,      2)
(0538,     12) (0b11,      1) (0c3b,      3) (0527,      5)
(0810,      2) (0498,     12) (0c26,     12) (0b0c,      3)
(0217,    202) (0602,      7) (04cb,      4) (0b18,     12)
(0b22,      5) (0cd4,      1) (0514,      9) (0811,      6)
(034c,      6) (0c36,      3) (0911,     94) (0516,     10)
(0c60,      2) (085a,      4) (0532,      1) (0cb6,      2)
(0807,      1) (0813,      5) (0cb8,      1) (0000,      0)
```

```
[AC-hidecmd]_display memory 64 core 0
Block Size     64         Free      7       Used   3820       Total   3827
-------------------------Block From     0-------------------------
(d0333b40, 02600000)  (d0333ba0, 02600000)  (d0333c00, 02600000)
(d0333c60, 011e0025)  (d0333cc0, 01101001)  (d0333d20, 01101001)
(d0333d80, 011e0025)  (d0333de0, 011e0025)  (d0333e40, 01106002)
(d0333ea0, 01109001)  (d0333f00, 01109001)
```

```
[AC-hidecmd]_display memory 128 group core 0
(cc00,      1) (cc03,      1) (0846,      2) (0801,     17)
(0802,     17) (0276,      1) (0110,     37) (0830,      2)
(0806,     22) (0214,    480) (0216,    500) (0b28,      1)
(0c43,      9) (0240,    106) (0d20,    452) (0b25,      1)
(0833,      1) (0310,      1) (0213,     34) (0218,      3)
(0278,      1) (0260,      1) (0490,      3) (0501,      4)
(0c71,     24) (0101,      2) (04a0,     12) (0102,      1)
(0125,      2) (0cb9,      3) (0cb6,      1) (0b0b,      2)
(011c,      2) (0ca0,     23) (0c11,     23) (0230,     19)
(0340,      2) (04c4,      2) (0468,      2) (0525,      2)
(0c14,      2) (0816,      2) (0b23,      2) (0b0c,      6)
(0b02,      1) (0900,      4) (0b01,      3) (0538,     10)
(041e,      8) (0527,      5) (0c2a,      7) (0000,      0)
```

```
[AC-hidecmd]_display memory 256 group core 0
(02f0,          1) (011c,          27) (0110,          2) (021b,          1)
(0830,          1) (0806,           2) (0213,        214) (0283,          1)
(0214,        850) (0125,         130) (040c,          1) (0b0c,          2)
(0101,         11) (04d2,          16) (0216,         78) (0c01,          1)
(010c,          1) (0c00,           2) (0240,         55) (042a,          1)
(0102,          3) (0c43,           2) (0425,          1) (0341,        501)
(0342,         91) (0523,           1) (0810,          1) (0320,         29)
(0c72,         13) (0c71,          21) (0420,          1) (0502,          1)
(0504,          1) (0491,           1) (0483,          1) (04a0,          7)
(043a,          1) (042e,           7) (0813,          1) (0869,          2)
(0807,          1) (0600,           1) (0661,          1) (0b05,        181)
(0b0b,          2) (0446,          23) (cc15,          2) (cc16,          5)
(041e,         16) (0467,           2) (0428,          2) (0c30,          6)
(0816,          1) (0b18,           1) (0846,          1) (0526,          5)
(0b01,          4) (0b02,           9) (0b11,          2) (0b23,          1)
(0b0d,          1) (0514,           1) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 512 group core 0
(0117,          1) (cc00,           1) (011e,          4) (0110,          7)
(0cb6,          1) (0813,           1) (0c43,         13) (0c00,          1)
(0c01,          1) (0341,           1) (0216,         28) (0360,          1)
(041e,          2) (04ca,           1) (04c9,          1) (0532,          1)
(0125,         10) (04d2,           1) (051d,          4) (0260,          2)
(0213,          3) (0230,           9) (040c,          1) (0342,         11)
(0c72,          3) (0240,          10) (0c0e,          1) (04a0,         23)
(04a6,          2) (0102,           3) (0869,          2) (0602,          1)
(0101,          1) (0b1a,           1) (0801,         16) (0501,          4)
(085a,         11) (0526,          10) (0b02,          5) (0278,          3)
(0d20,         68) (0b01,           2) (0214,        205) (0217,         20)
(0c2b,          1) (0000,           0) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 1024 group core 0
(0118,          1) (010d,           1) (0160,          5) (0110,         38)
(021b,          1) (085f,           1) (0216,        108) (0c71,          1)
(021c,          4) (0215,        1004) (0cb8,          1) (0101,          3)
(0602,          2) (011e,           1) (0cb6,          1) (0900,          1)
(041e,          1) (051c,           1) (0508,          1) (0b28,          4)
(0b01,          1) (0d10,           1) (0509,          8) (04d2,          2)
(0518,         10) (0b0b,           1) (cc16,         10) (0320,          5)
(0b11,          1) (cc15,           2) (04a0,          4) (0102,          4)
(011c,          1) (0490,           3) (0214,          3) (0264,          1)
(0260,          1) (0b13,           1) (0b18,          2) (0213,          1)
(0b05,         68) (040c,           1) (0b02,         14) (0d20,          1)
(0217,        139) (0278,           2) (0000,          0) (0000,          0)
```

```
[AC-hidecmd]_display memory 2048 group core 0
(0118,        1) (0101,       10) (0102,       46) (0110,        2)
(010f,        2) (0821,        5) (021b,        1) (0283,       14)
(0111,        1) (0d10,        1) (0125,        8) (0218,       10)
(0260,        1) (0216,       10) (0264,        1) (042a,        1)
(0341,        3) (040c,        1) (0342,        5) (0425,        1)
(0cc5,        1) (0661,        2) (0420,        5) (0502,        1)
(0504,        1) (0491,        1) (04a0,       16) (cc16,        5)
(043a,        1) (0523,        1) (042e,        1) (0805,        5)
(0813,        1) (0807,        1) (0cb6,        1) (0602,        6)
(0000,        2) (0600,        7) (ccc8,        1) (0810,        2)
(011c,        1) (0525,        2) (011e,        1) (0526,        2)
(0217,        1) (0278,        1) (0000,        0) (0000,        0)
```

```
[AC-hidecmd]_display memory 4096 group core 0
(0160,        1) (010f,        1) (0110,        1) (0822,        1)
(0813,        2) (0821,        1) (01ff,     1381) (0111,      200)
(0c43,       18) (0102,        8) (0b02,        4) (0101,        9)
(0b28,        1) (0b01,        1) (0911,        1) (0216,       13)
(0c44,        1) (0230,        2) (0342,        1) (0321,        4)
(0501,        1) (0517,        2) (011e,        2) (0537,        1)
(0516,        1) (04a0,       10) (0805,        5) (011c,        1)
(0602,        9) (0c60,        2) (0b0b,        1) (0b13,        1)
(0240,        2) (ccc8,        1) (0509,        2) (0816,        1)
(0c28,        3) (0514,        1) (0000,        0) (0000,        0)
```


李晨光
表示上一步结果正常
表示上一步结果出现问题
开始
是否热重启
AC异常重启故障排查
故障前有无人员操作设备
检查电源状况
了解近期网络割接、配置变更情况
收集信息
拨打热线
400-810-0504寻求帮助

1. 开始

AC 重启的原因总共有几种情况：①电源问题；②手动 reboot；③软件错误导致的内存异常重启；④CPU 死循环触发软件看门狗保护重启；⑤CPU 硬件重启等。

定位故障的思路是：先排除电源掉电和人为手动重启的可能性，对于其他可能原因需要尽可能多的收集信息辅助 H3C 工程师定位。

2. 流程图相关操作说明

（1）是否热重启

① 通过网管确定是否热重启。如果 AC 有纳入网管，AC 重启的告警信息会送到网管平台。通过网管收集的告警信息就能准确确定重启时间、次数以及重启类型是热重启还是冷重启。

例如：IMC 平台收到冷启动告警，如图 7-1 所示。



图 7-1 IMC 平台收到冷启动告警

AC 热重启、冷重启的告警 OID 分别如表 7-2 所示。

表 7-2 AC 热重启、冷重启的告警 OID

Trap 中文名称	Trap 名称	OID
系统冷启动通告	hwSysColdStartTrap	1.3.6.1.4.1.2011.10.6.8.4
系统热启动通告	hwSysWarmStartTrap	1.3.6.1.4.1.2011.10.6.8.5

② 通过 AC 命令行确定是否热重启。在 AC 上也能通过命令查看 AC 上一次重启类型。

命令：*display reboot-type*

例如：上次重启类型为 Cold 属于冷重启，如果为 Warm 则属于热重启。

```
<AC>display reboot-type
  The rebooting type this time is:Cold
```

(2) 检查电源状况

冷重启一般和电源掉电、板卡插拔等操作相关。所以主要检查电源供电状况以及机房近期有无施工导致断电情况。

如果是插卡式 AC,可以查看同机框的其他板卡在同一时刻有无重启现象,或者检查交换机信息也可以辅助定位电源问题。

(3) 故障前有无人员操作设备

查看有无人员操作设备和做了哪些操作。

① 是否使用了命令行、Web 操作或者网管 set 相关 OID 等操作主动对设备进行了重启,要先予以排除。

② 收集 AC 硬件记录的信息来辅助判断人为的主动重启。

命令:*display reboot-information from-device 5*

例如:通过 Web、网管、Telnet 命令行方式重启 AC 时,硬件记录信息如下。

```
[AC-hidecmd]display reboot-information from-device 5

---------------- Reboot info ----------------
nReboot Task:                HDQ0 (TID: 89)         //web 方式重启
nReboot Time:                2013-04-23  15:14:29
nReboot Tick:                0x31(CPU Tick High) 0xc1c08ab7(CPU Tick Low)
nReboot Type:                WARM

---------------- Reboot info ----------------
nReboot Task:                STMR (TID: 5)          //网管重启
nReboot Time:                2013-04-23  15:41:51
nReboot Tick:                0x18(CPU Tick High) 0x56459987(CPU Tick Low)
nReboot Type:                WARM

---------------- Reboot info ----------------
nReboot Task:                vt0 (TID: 86)          //telnet 命令行重启
nReboot Time:                2013-04-23  14:12:18
nReboot Tick:                0xe1(CPU Tick High) 0xa2cb9302(CPU Tick Low)
nReboot Type:                WARM
```

(4) 收集信息

① 如果有日志服务器,收集 Log 服务器上的日志信息。

② 收集 AC 设备上信息,反馈 H3C 工程师定位。

第一,hidecmd 隐含模式收集(系统视图下通过_hidecmd 命令进入)。

display cpu-usage history　　　　//隔 10 秒钟收集一次,共 5 次。

display cpu-usage task　　　　//隔 10 秒钟收集一次,共 5 次。

display task　　　　//隔 10 秒钟收集一次,共 5 次。

display reboot-informationverbose from-device 5

第二,diagnose 诊断模式收集(在 hidecmd 隐含模式通过 en_diag 命令进入)。

diag boot-info display

第三，系统模式收集。

display device manuinfo

display diagnostic-information　　　//隔 1 分钟收集 1 次，共收集 2 次。

AC R2308P10(内部版本号 B96D023SP01)之前版本还需收集。

hidecmd 隐藏模式下收集(系统视图下通过_hidecmd 命令进入)。

display reboot-type

display exception 10 verbose from-device

display deadloop 20 verbose from-device

display queue

fpl-diag enable　　　//命令直接打全，Tab 键不能补全。

fpl-diag showexception　　　//命令直接打全，Tab 键不能补全。

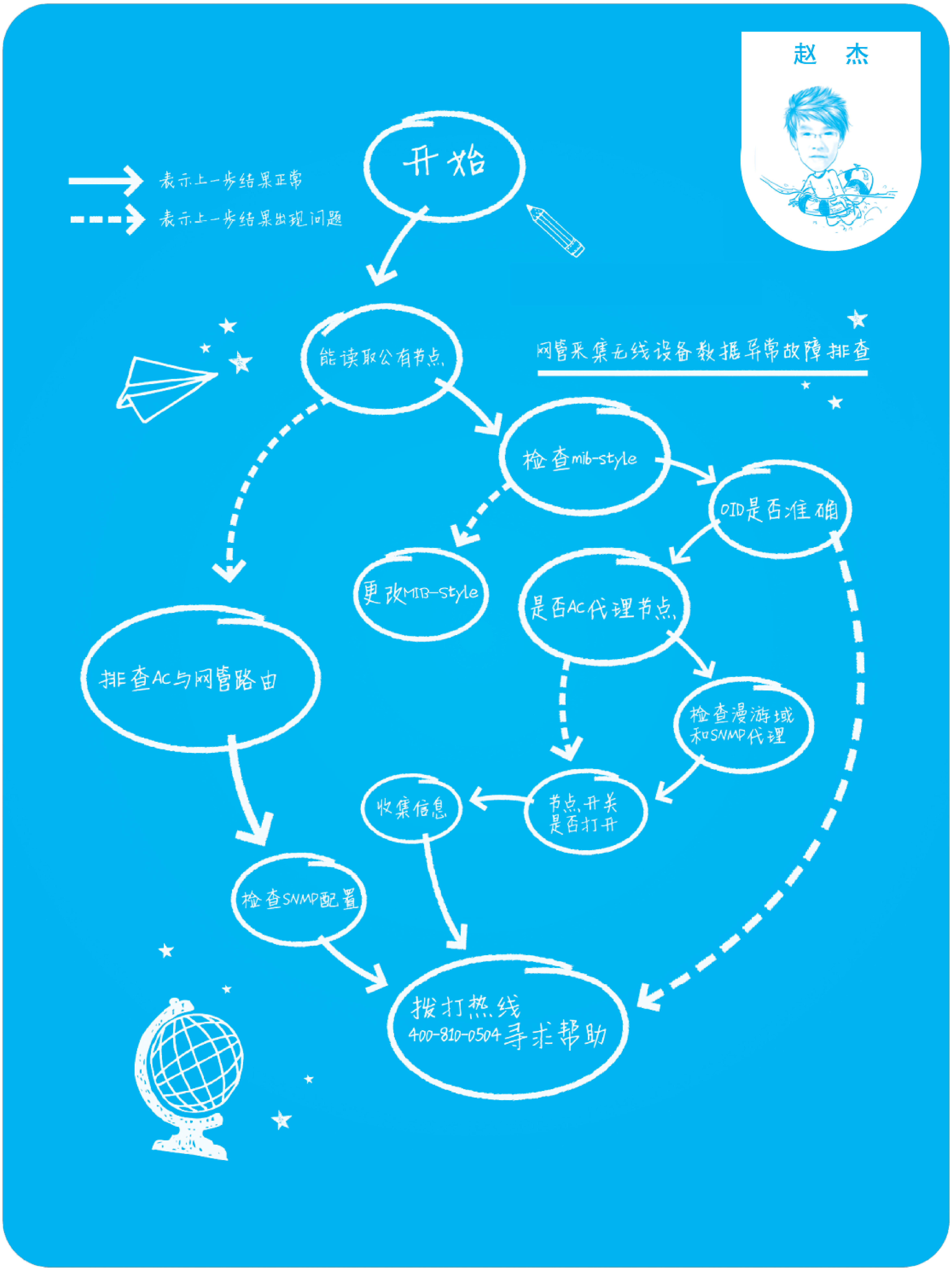
fpl showcpufc　　　//命令直接打全，Tab 键不能补全。

fpl showmem　　　//命令直接打全，Tab 键不能补全。

(5) 了解近期网络割接、配置变更情况

如果近期有人员登录设备，则需要尽可能丰富地了解其操作方式、配置变更情况。关于现网的其他割接动作也尽可能收集信息，比如新业务开通、业务变更等。这些都能辅助 H3C 工程师快速定位问题。

信息反馈 H3C 工程师后，再一起探讨，共商处理策略。


赵 杰
表示上一步结果正常
表示上一步结果出现问题
开始
网管采集无线设备数据异常故障排查
能读取公有节点
检查mib-style
OID是否准确
更改MIB-style
是否AC代理节点
排查AC与网管路由
检查漫游域和SNMP代理
节点开关是否打开
收集信息
检查SNMP配置
拨打热线
400-810-0504寻求帮助

07 无线产品 > 7.1 AC > 7.1.4 网管采集无线设备数据异常故障排查 > 步骤详解

1. 开始

网管软件采集无线设备节点使用 SNMP 协议，无线设备对于网管采集有认证和接入权限控制，网管采集无线设备上部分节点时，需要开启相应的采集开关。

网管采集故障排查思路：首先检查读取设备公有节点情况，其次检查设备 MIB-Style，然后检查是否为 AC 代理节点，最后排查节点是否有统计开关。

2. 流程图相关操作说明

(1) 能读取公有节点

设备节点包括公有节点和私有节点，网管通过 SNMP 协议与无线设备连接成功后，可以采集公有节点数据，采集私有节点受到设备 MIB-Style、AC 代理、统计开关等因素影响，如果采集不到私有节点数据，请参考后续排查思路。使用 MIB Browser 采集举例如下。

采集设备名称(公有)：1.3.6.1.2.1.1.5，如图 7-2 所示。

采集上线 AP 数量(私有)：1.3.6.1.4.1.**2011.10**.2.75.1.1.2.1，如图 7-3 所示。

```
***** SNMP QUERY STARTED *****
1: sysName.0 (octet string) AC2 [41.43.32 (hex)]
***** SNMP QUERY FINISHED *****
```

图 7-2　采集设备名称

```
***** SNMP QUERY STARTED *****
1: h3cDot11APConnectCount.0 (integer) 1
***** SNMP QUERY FINISHED *****
```

图 7-3　采集上线 AP 数量

(2) 检查 MIB-Style

设备 MIB-Style 有 New 模式和 Compatible 模式，无线设备常用 Compatible 模式。与网管确定其所要读取的 OID 节点，根据 OID 节点判断 H3C 设备应该使用哪种模式。例如网管需要读取的是：1.3.6.1.4.1.**25506**.2.6.1.1.1.1.8，则 H3C 设备对应的 MIB-Style 为 New 模式；如果网管读取节点为：1.3.6.1.4.1.**2011.10**.2.6.1.1.1.1.8，则 H3C 设备对应的 MIB-Style 为 Compatible 模式。

命令：*display mib-sytle*

例如：通过命令查看设备当前的 MIB-Style，网管采集节点对应模式与设备当前模式一致，才能正常采集数据。

```
[AC]display mib-style
 Current MIB style:compatible
 Next reboot MIB style: compatible
```

(3) OID 是否准确

通过节点名称或者 OID 在《无线产品支持 MIB 清单 AC》中查找满足网管需求的节点。

(4) 是否 AC 代理节点

了解当前组网情况，AC+IAG 组网情况下，AC 可以代理读取 IAG 数据，采集节点是 AC 代理节点，需要配置漫游域和 SNMP 代理。如果节点在《无线产品支持 MIB 清单 AC》"AC-BAS 一体化"表中，则节点属于代理节点。

(5) 检查漫游域和 SNMP 代理

AC+IAG 组网模式下，采集 AC 代理节点数据需要配置漫游域和 SNMP 代理。

命令：*display current-configuration configuration* | *include snmp*

display wlan mobility-group

例如：通过命令查看SNMP代理配置以及AC与IAG之间的漫游域状态如下。

① 检查设备SNMP代理配置。

```
[AC]display current-configuration configuration | include snmp
 snmp-agent proxy ip 192.168.2.102
 snmp-agent
 snmp-agent local-engineid 800063A2033822D6D74AF1
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version v2c
 snmp-agent target-host trap address udp-domain 192.168.2.253 params securityname public v2c
```

② 检查漫游域状态。

```
[AC]display wlan mobility-group
                        Member Information
--------------------------------------------------------------------------
 IP Address                 : 192.168.2.102
 State                      : Run
 Interface                  : WLAN-Tunnel0
 Online Time (hh:mm:ss)     : 00:07:32
--------------------------------------------------------------------------
```

③ 查看漫游域配置。

```
[AC]wlan mobility-group 1
memberip 192.168.2.102                  #对端设备互通IP
sourceip 192.168.2.100                  #本端设备互通IP
mobility-group enable                   #使能漫游域
```

（6）节点开关是否打开

① 查询节点周期控制列表。采集部分节点需要配置特定的统计周期，采集节点与统计开关的对应关系请参考《无线产品支持MIB清单 AC》中周期控制列表。

例如：AP接收平均信号强度(1.3.6.1.4.1.2011.10.2.75.2.1.3.1.19)，采集数据需要配置采集周期如下。

hwSysStatisticPeriod(1.3.6.1.4.1.2011.10.6.11.1)

hwSysSamplePeriod(1.3.6.1.4.1.2011.10.6.11.2)

如果未配置采集周期，采集的数据是固定数值——120。

```
 ***** SNMP QUERY STARTED *****
1: h3cDot11AvgRxSignalStrength.20.50.49.57.56.48.49.65.48.68.49.67.49.50.51.48.50.51.55.
48.51.1 (integer) 0
2: h3cDot11AvgRxSignalStrength.20.50.49.57.56.48.49.65.48.68.49.67.49.50.51.48.50.51.55.
48.51.2 (integer) -120
 ***** SNMP QUERY FINISHED *****
```

配置采集周期后，采集数值随着采集周期变化，本次采集数值——57。

```
***** SNMP QUERY STARTED *****
1: h3cDot11AvgRxSignalStrength.20.50.49.57.56.48.49.65.48.68.49.67.49.50.51.48.50.51.55.
48.51.1 (integer) 0
2: h3cDot11AvgRxSignalStrength.20.50.49.57.56.48.49.65.48.68.49.67.49.50.51.48.50.51.55.
48.51.2 (integer) -57
***** SNMP QUERY FINISHED *****
```

② 配置采集周期。通过网管配置采集周期，等待一个统计周期后，网管可以采集相关节点数据。

例如：节点 AP 接收平均信号强度(1.3.6.1.4.1.2011.10.2.75.2.1.3.1.19)，需要配置统计周期和采集周期，通过网管 set 操作配置。

```
***** SNMP SET-RESPONSE START *****
1: hwSysStatisticPeriod.0 (integer) 9
***** SNMP SET-RESPONSE END *****
***** SNMP SET-RESPONSE START *****
1: hwSysSamplePeriod.0 (integer) 3
***** SNMP SET-RESPONSE END *****
```

(7) 排查 AC 与网管路由

此步骤可以通过网管 ping AC。检查 AC 与网管之间的链路情况，注意链路要支持 MTU 1500。

命令：*ping -s 1472 -f x.x.x.x*

例如：ping 1472 字节包(MTU 1500)，强制不分片，检测网管到 AC 链路。

```
<AC>ping -s 1472 -f 192.168.2.253
  PING 117.130.195.46:1472  data bytes, press CTRL_C to break
    Reply from192.168.2.253: bytes=1472 Sequence=1 ttl=21 time=20 ms
    Reply from192.168.2.253: bytes=1472 Sequence=2 ttl=21 time=20 ms
    Reply from192.168.2.253: bytes=1472 Sequence=3 ttl=21 time=20 ms
    Reply from192.168.2.253: bytes=1472 Sequence=4 ttl=21 time=20 ms
```

(8) 检查 SNMP 配置

SNMP V2/V3 版本对网管有认证要求，设备使用 ACL 配合 SNMP 协议可以实现接入权限控制。

① SNMP 接入认证。

命令：*display current-configuration configuration | include snmp*

例如：通过命令查看设备 SNMP 读写团体名以及设备当前运行的 SNMP 版本。

```
[AC]display current-configuration configuration |include snmp
 snmp-agent proxy ip 192.168.2.102
 snmp-agent
 snmp-agent local-engineid 800063A2033822D6D74AF1
 snmp-agent community read public acl 2001
 snmp-agent community write private acl 2001
 snmp-agent sys-info version v2c
```

② 接入权限控制。

命令：*display acl xxxx*

例如：SNMP 协议结合 ACL 实现网段控制权限，查看设备配置的 SNMP 接入权限。

```
[AC]display current-configuration configuration |include snmp
 snmp-agent proxy ip 192.168.2.102
 snmp-agent
 snmp-agent local-engineid 800063A2033822D6D74AF1
 snmp-agent community read public acl 2001
 snmp-agent community write private acl 2001
 snmp-agent sys-info version v2c
[AC]display acl 2001
BasicACL  2001, named mib_1, 1 rule,
ACL's step is 5
 rule 1 permit source 192.168.2.103 0
```

（9）更改 MIB-Style

设备支持 New 模式和 Compatible 模式，通过命令可以切换两种模式，如果更改设备的 MIB 模式，需要重启设备生效。

命令：*mib-style compatible*

例如：设备工作在 New 模式，通过命令修改，重启后为 Compatible 模式。

```
[AC]mib-style ?
  compatible   Compatible style MIB
  new          New style MIB
[AC]mib-style compatible
```

（10）收集信息

如果按照上述排查步骤不能解决故障，请收集以下信息反馈给 H3C 售后技术人员处理。

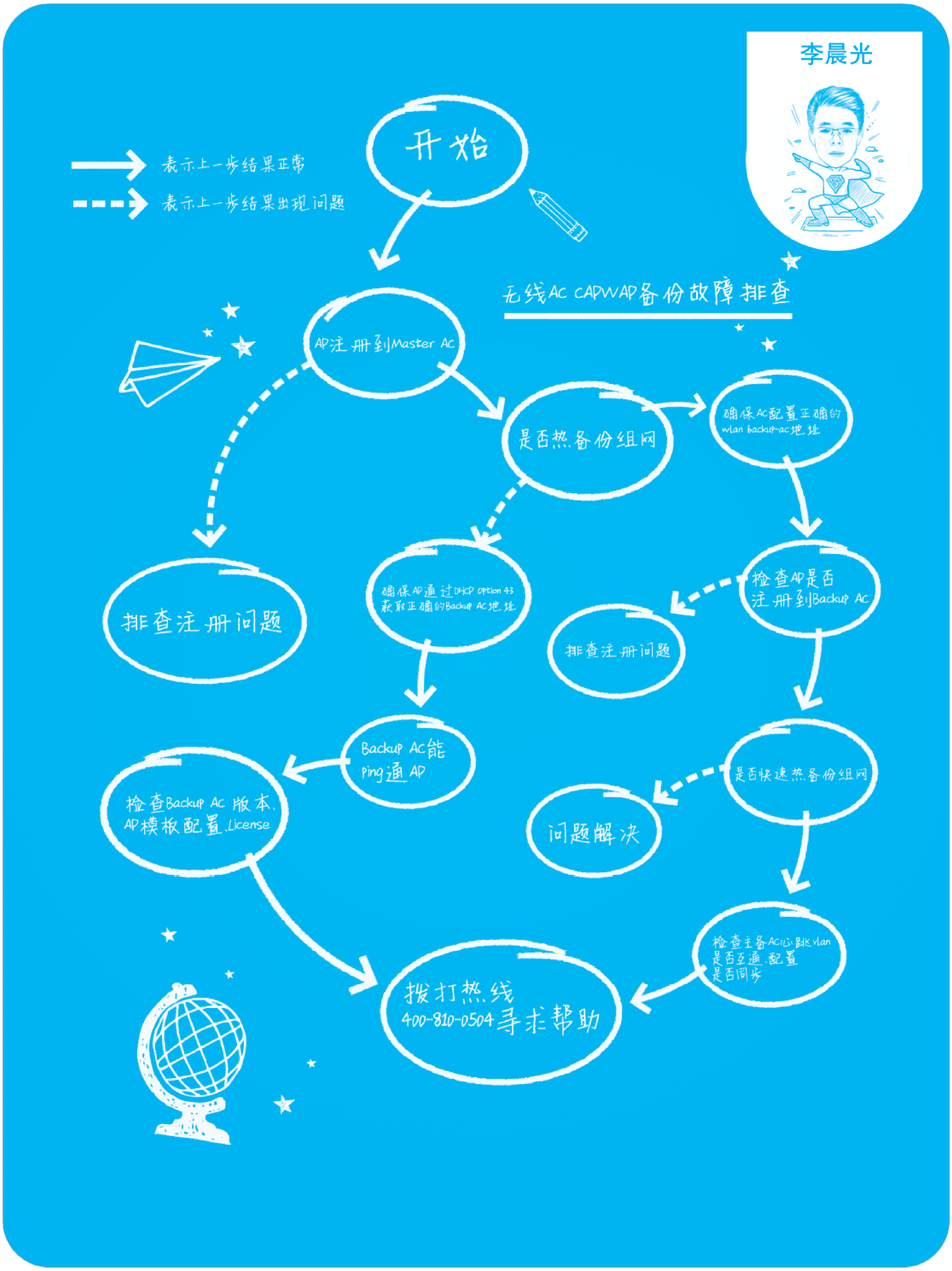
① 采集有问题的节点 OID。

② 设备配置。

```
<AC>displaycurrent-configuration
<AC>display mib-style
```

③ 调试信息，收集调试信息前，查看当前 CPU 利用率和内存利用率，并反馈技术人员判断是否可以收集调试信息。

```
<AC>debugging snmp agent packet send
<AC>debugging snmp agent packet receive
```


李晨光
无线AC CAPWAP备份故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
AP注册到Master AC
排查注册问题
是否热备份组网
确保AC配置正确的
wlan backup-ac地址
确保AP通过DHCP option 43
获取正确的Backup AC地址
检查AP是否
注册到Backup AC
排查注册问题
Backup AC能
ping通 AP
检查Backup AC 版本、
AP模板配置、License
是否快速热备份组网
问题解决
检查主备AC心跳vlan
是否互通、配置
是否同步
拨打热线
400-810-0504寻求帮助

1. 开始

AC-AP 隧道备份主要以瘦 AP 注册 AC 为基础，故障排查方法根据是否热备份、快速热备份等不同组网需求而略有差异。定位故障的思路是：先保证 AP 注册 Master AC，再确保 AP 能获取正确的 Backup AC 地址，成功注册 Backup AC，最后考虑快速热备、心跳等。

N+1 备份按冷备份方式排查。另外，本流程图针对 AP 的双隧道备份问题，不涉及 Portal、802.1x 认证等业务备份。

2. 流程图相关操作说明

(1) AP 注册到 Master AC

无线 AC 的 Master or Backup 是以 AP 为参照对象定义的，即某一台 AC 可能属于 AP1 的主用控制器，又可能同时属于 AP2 的备份控制器。一般的，配置某 AP 的注册优先级为 7 的 AC 为该 AP 的主用控制器。AP 成功注册 Master AC 是备份排查第一步。

检查 AP 在 Master AC 上的注册状态如下。

命令：*display wlan ap all*

例如：State 为“I”表示 AP 未上线；State 为“R/M”“R/B”表示已上线，分别为主、备隧道。

```
<H3C>display wlan ap all
State :I = Idle,     J = Join, JA = JoinAck,     IL = ImageLoad
       C = Config, R = Run,    KU = KeyUpdate, KC = KeyCfm
------------------------------------------------------------------------------------
 AP Name                        State  Model                 Serial-ID
------------------------------------------------------------------------------------
 fz_dgl_001                     I      WA1208E-GP            210235A0A9C094001953
 fz_dgl_002                     R/M    WA1208E-GP            210235A0A9C094001529
 fz_dgl_003                     R/B    WA2100                210235A22WB093001434
```

(2) 排查注册问题

若 AP 无法注册 Master AC，则按云图——《瘦 AP 注册不上问题排错》标准流程图处理。

(3) 是否热备份组网

根据用户实际组网情况确定 AC 备份方式，即冷备份还是热备份。

对于冷备份情况下，AP 在正常情况下只与 Master AC 建立主 CAPWAP 隧道，只有当主隧道断开后，才向 Backup AC 发起注册请求，建立备 CAPWAP 隧道。对于热备份情况，AP 会同时与 Master AC 和 Backup AC 建立 CAPWAP 隧道，但业务数据只转发到 Master AC。

(4) 确保 AP 通过 DHCP Option 43 获取正确的 Backup AC 地址

冷备情况下，AP 一般通过 DHCP Option 43 获取 Backup AC 地址，请检查 DHCP Server Option 43 配置。

命令：*display dhcp server tree all*

```
<H3C>display dhcp server tree all
Global pool:

Pool name: 1
```

```
network192.168.86.0 mask 255.255.255.0
 Sibling node:2
 gateway-list 10.21.101.1
 option 43 hex 800B0000 020A1564 030A1564 07
 expired 10 0 0
```

附 Option 43 格式简要说明如图 7-4 所示。

```
80 0B 00 00 02 0A 15 64 03 0A 15 64 07
80：固定值，不用改变；
0B：长度字段，其后面所跟数据的字节长度；
00 00：固定值，不用改变；
02：表示后面的 IP 地址的个数，此处为二个 IP 地址；
0A 15 64 03：十六进制转十进制为 IP 地址一 10.21.100.3
0A 15 64 07：十六进制转十进制为 IP 地址二 10.21.100.7
```

图 7-4　Option 43 格式简要说明

注意：当修改 DHCP Server 配置后，需要让 AP 重新获取地址，新配置才能生效。

(5) Backup AC 能 ping 通 AP

在备份 AC 上指定源地址(Option 43 指定的接口地址)ping AP 来测试。需要注意的是，CAPWAP 隧道对 AP-AC 之间的链路丢包比较敏感，要求有线丢包率小于 0.1%。同时链路要支持 MTU 1500。

命令：*ping -a x.x.x.x*(AC 注册地址) *-s 1472 -f x.x.x.x*(AP 地址)

例如：ping 1472 字节包(MTU 1500)，强制不分片，检测 AP-AC 链路。

```
<AC-Backup>ping -a 10.21.100.7 -s 1472 -f 192.168.86.46
  PING192.168.86.46: 1472   data bytes, press CTRL_C to break
    Reply from192.168.86.46: bytes=1472 Sequence=1 ttl=21 time=20 ms
    Reply from192.168.86.46: bytes=1472 Sequence=2 ttl=21 time=20 ms
    Reply from192.168.86.46: bytes=1472 Sequence=3 ttl=21 time=20 ms
    Reply from192.168.86.46: bytes=1472 Sequence=4 ttl=21 time=20 ms
```

如果 AP 到 Backup AC 无法 ping 通，则需要排查网络连通性。

(6) 检查 Backup AC 版本、AP 模板配置、License

① 检查主、备 AC 软件版本是否一致。

命令：*_display version*

```
<Backup-AC>_display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 2308P10
Comware Platform Software VersionCOMWAREV500R002B96D323SP01
EWPX2WCMD0 Software Version V200R003B96D023SP01
Copyright (c) 2004-2012 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
Compiled Aug 31 2012 16:04:14, RELEASE SOFTWARE
EWPX2WCMD0 uptime is 16 weeks, 6 days, 14 hours, 4 minutes
```

② 查看 AP 模板配置。

命令：*display current-configuration*

例如：检查 AP 型号、序列号配置，确保跟 AP 的实际序列号一致。

```
<AC-Backup>display current-configuration
#
wlan apfz_dgl_001 model WA1208E-GP id 76
 priority level4
 serial-id210235A0A9C094001953
 radio 1
```

另外，如果 AP 通过 MAC 地址信息注册 AC，此时需要确保 AP MAC 地址信息正确。

```
<AC-Backup>display current-configuration
#
wlan apfz_dgl_001 model WA1208E-GP id 76
 priority level4
 serial-id0023-8999-fec0
 radio 1
```

③ 检查 Backup AC License。查看备 AC License，对比备 AC 上 AP 注册数目，确定是否需要 License 扩容。

第一，检查备 AC License 所支持的 AP 注册数量。

命令：*display license ap*

```
<AC>display license ap
No. Serial number                                   AP Number    Available Time Left
--------------------------------------------------------------------------------
 1  ZrxbR-5nHmt-$C&tn-acm55-q&qSN-D+:K3-b9EFH          128        Forever
 2  yb@Cc-LNw4c-dYGr9-hxe$r-kr/k4-Cj3s3-@/hcq          128        Forever
 3  uc$tS-wJk3q-rKrc+-$Eq9n-F6inS-+U5&z-2K4gg          128        Forever
```

计算公式：

$$\text{AC 支持的 AP 注册数量} = \text{该型号 AC 默认规格} + \sum \text{每条 License 步长}$$

注意：当 AC 添加 License 后，需要重启 AC，该 License 才能生效。

第二，检查备 AC 当前已经注册的 AP 数量。

命令：*display wlan ap all*

```
<AC> display wlan ap all
 Total Number of APs configured              : 729
 Total Number of configured APs connected    : 613
 Total Number of auto APs connected          : 0
```

计算公式：

AP 当前注册数量 ="Total Number of configured APs connected"
+"Total Number of auto APs connected"

第三，对比确认是否需要对 License 扩容。

比较"AC 支持的 AP 注册数量"和"AP 当前注册数量"，如果二者相等，则说明备 AC License 达到允许注册的 AP 数上限，AC 需要 License 扩容。

(7) 确保 AC 配置正确的 WLAN Backup-AC 地址

热备情况下，AP 只能通过 Master AC 的配置信息获取 Backup AC 地址。AC 配置 Backup-AC 地址有两种方式。

① 全局指定。

```
<H3C> displaycurrent-configuration
 #
wlan backup-ac ip 10.21.100.7
```

② 在 AP 模板下指定。

```
<H3C> displaycurrent-configuration
 #
wlan apfz_dgl_001 model WA1208E-GP id 76
 priority level 7
 serial-id210235A0A9C094001953
 backup-ac ip 10.21.100.7
 radio 1
```

第二配置方式优先级高。

注意：备 AC 上同样需要配置 Backup-AC IP 为主 AC 的 CAPWAP 隧道接口地址。

(8) 检查 AP 是否注册到 Backup AC

热备情况下，当 AP 获取了 Backup AC 地址后，就会向 Backup AC 发起注册请求。

检查瘦 AP 在备 AC 注册状态如下。

命令：*display wlan ap all*

例如：State 为"I"表示 AP 未上线；State 为"R/M""R/B"表示已上线，分别为主、备隧道。

```
<H3C>display wlan ap all
State :I = Idle,    J = Join, JA = JoinAck,    IL = ImageLoad
          C = Config, R = Run,   KU = KeyUpdate, KC = KeyCfm
--------------------------------------------------------------------------------
 AP Name                        State  Model              Serial-ID
--------------------------------------------------------------------------------
 fz_dgl_001                     I      WA1208E-GP         210235A0A9C094001953
 fz_dgl_002                     R/M    WA1208E-GP         210235A0A9C094001529
 fz_dgl_003                     R/B    WA2100             210235A22WB093001434
```

(9) 排查注册问题

若仍无法注册 Backup AC，按云图《瘦 AP 注册不上问题排错》标准流程图处理。

(10) 是否快速热备份组网

根据用户实际组网情况确定 AC 热备份方式，是普通热备份还是快速热备份。

快速热备份中"快速"是相对于 AP 主、备切换的快慢而言的。普通热备中，AP 通过 AP-AC 间心跳机制维持 CAPWAP 隧道(10s 一次心跳，3 次超时判断隧道断开)，当 AP 检测到主隧道断开时，数据转发才开始切换到备份隧道，这个切换时延需要大约 30s。

快速热备中，Master AC、Backup AC 之间通过热备心跳机制确保对方工作正常(参数可调，默认 2s 一次心跳，3 次超时判断对方 AC 不可用)，当 Backup AC 检测到 Master AC 不可用时，会立刻通知 AP 切换 CAPWAP 隧道，切换时延可以达到毫秒级。

(11) 问题解决

当 AP 能成功注册 Backup AC，且组网不要求快速热备份，则问题已经解决完成。

(12) 检查主备 AC 心跳 VLAN 是否互通、配置是否同步

快速热备情况下，首先需要保证主备 AC 在心跳 VLAN 内二层互通。其次需要保证主、

备 AC 配置同步，比如指定相同的心跳参数，配置相同的 WLAN rrm 参数，AP 射频下绑定相同的服务模板。

① 心跳 VLAN 互通性测试方法。可以通过在 AC 起三层接口 ping 包来测试热备心跳链路质量，保证无丢包和超过 1s 的延迟抖动。

② 检查主备 AC 配置是否同步。

```
<AC>display current-configuration
#
 hot-backup enable domain 1
 hot-backup vlan 4002
 hot-backup hellointerval2000
#
```

```
<AC-Backup>display current-configuration
#
 hot-backup enable domain 1
 hot-backup vlan 4002
 hot-backup hellointerval2000
#
```

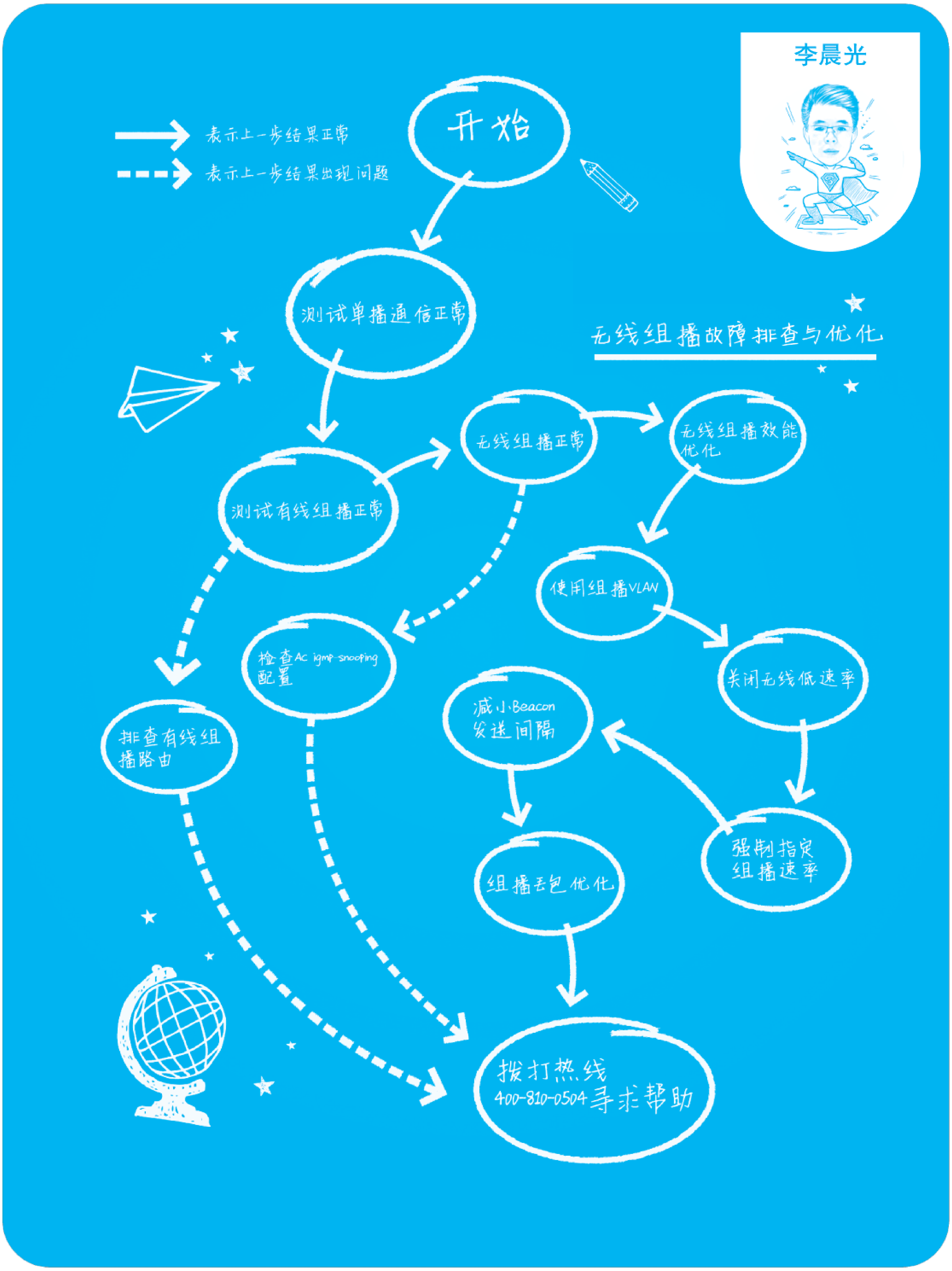
③ 查看热备是否生效。AC 的快速热备份是否生效可以通过命令行来查看。

命令：*display hot-backup state*（系统模式下）

例如：在主、备 AC 上查看热备状态。

```
[AC]display hot-backup state
*******************************************************************
Vlan ID                 : 9
Domain ID               : 1
Link State              : Connect
Peer Board MAC          : 3822-d626-da14
Peer Board State        : Normal
Hello Interval          : 150

[AC-Backup]display hot-backup state
*******************************************************************
Vlan ID                 : 9
Domain ID               : 1
Link State              : Connect
Peer Board MAC          : 3822-d626-da23
Peer Board State        : Normal
Hello Interval          : 150
```


李晨光
无线组播故障排查与优化
表示上一步结果正常
表示上一步结果出现问题
开始
测试单播通信正常
测试有线组播正常
无线组播正常
无线组播效能优化
使用组播VLAN
关闭无线低速率
强制指定组播速率
减小Beacon发送间隔
组播丢包优化
检查Ac igmp-snooping配置
排查有线组播路由
拨打热线
400-810-0504寻求帮助

1. 开始

在无线组播应用中，无线设备包括 AC 仅做本地的二层组播转发，本身并不支持组播路由。

所以定位故障的思路是：先确保 AC 上联有线网络组播路由互通，再排查 AC 的无线二层组播并做相应的优化。

2. 流程图相关操作说明

（1）测试单播通信正常

确保客户端到服务器单播路由可达，如图 7-5 所示，这是组播处理的前提。

命令：*ping -l 1500 x.x.x.x*



图 7-5　客户端到服务器单播路由

如果单播不通，请排查组播客户端到组播服务器单播路由。

（2）测试有线组播正常

本步骤确定 AC 上行有线网络组播路由互通。

测试方法：可以通过有线网络组播业务验证来测试组播路由互通性，即组播客户端直连有线，替代 AC 位置测试有线组播应用。

说明：AC 仅支持二层的组播转发，有线组播互通是无线组播处理的前提。

（3）排查有线组播路由

如有线组播业务不通，需排查有线组播路由或者组播服务器、客户端设置。

检查 IGMP 查询器配置：由于 AC 不支持组播路由，因此必须有其他三层设备将组播数据引入本地网，这就是 IGMP 查询器 Router。

三层交换机上配置 IGMP 查询器举例如下。

```
<H3C-SW>display current-configuration
 #
multicast routing-enable                //使能组播路由
 #
interface Vlan-interface2
 ip address 192.168.2.101 255.255.255.0
 IGMP enable
 IGMP version2
 pim sm                                 //组播业务 vlan 使能 IGMP 必须同时使能 pim
 #
```

(4) 无线组播正常

无线组播客户端接入无线网络后访问组播服务器资源。AC 上查看组播组信息应该能看到组播成员端口加入。

命令：*display IGMP-snooping group*

```
<H3C>display IGMP-snooping group
  Total1 IP Group(s).
  Total1 IP Source(s).
  Total1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total1 IP Group(s).
    Total1 IP Source(s).
    Total1 MAC Group(s).
    Router port(s):total 1 port(s).
            BAGG1                          (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (0.0.0.0, 224.1.1.1):
          Host port(s):total 1 port(s).
            WLAN-DBSS2:2                   (D)
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port(s).
            WLAN-DBSS2:2
```

(5) 检查 AC IGMP-Snooping 配置

AC 全局开启 IGMP-Snooping，相应组播业务 VLAN 使能 IGMP-Snooping。

```
<AC>display current-configuration
#
IGMP-snooping
#
vlan 2
 IGMP-snooping enable
 IGMP-snooping querier
 IGMP-snooping general-query source-ip current-interface
#
```

说明：如果是纯二层组播应用，即组播服务器和组播客户端同处二层网。AC 还需要承担查询器角色。可以在 AC 设备上使能 IGMP-Snooping 查询器，使 AC 能够在二层网络建立并维护组播转发表项，从而正常转发组播数据。

```
<AC>display current-configuration
#
IGMP-snooping
#
vlan 2
 IGMP-snooping enable
 IGMP-snooping querier
 IGMP-snooping general-query source-ip current-interface
#
```

(6) 无线组播效能优化

当组播业务数据基本可用后,下一步需要优化无线组播应用,以提升无线空口对组播的承载容量和终端体验。

一般情况下,无线组播的优化以常规的无线网络优化为基础,比如合理的信号部署,控制每个 AP 的用户数量,二层隔离等。无线网络优化是一套系统工程,有 H3C 专业团队提供支撑,如有 WLAN 网络专业优化服务的需求,请咨询 H3C 官方网站。

以下步骤对组播优化的专用手段做介绍。

(7) 使用组播 VLAN

当一个 AP 上连接的无线客户端可能位于多个 VLAN 的时候,而且这些客户端都在使用相同的组播组应用时,可以使用组播 VLAN 特性,目的是让组播数据只在组播 VLAN 内发送,防止同一份组播数据在无线空口被发送多次,影响空口性能。

```
<AC>display current-configuration
#
multicast-vlan 30                          //组播 VLAN 30
#
interface WLAN-ESS4
port link-type hybrid                      //必须为 hybrid 接口
port hybrid vlan 1 to 3 30 untagged        //组播 VLAN 30 必须被接口允许
mac-vlan enable
port multicast-vlan 30                     //接口增加到组播 VLAN 中
#
```

(8) 关闭无线低速率

对于 11g 的网络可以直接将 1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps 速率禁用,对于 11a 的网络可以直接将 6Mbps、9Mbps 速率禁用,这样整体上减少广播报文和管理报文对空口资源的占用。

在 WLAN rrm 视图使用 Disabled-Rate 命令关闭 1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps 速率。

```
<AC>display current-configuration
#
wlan rrm
 dot11a mandatory-rate 12 24
 dot11a supported-rate 18 36 48 54
 dot11a disabled-rate 6 9
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 11
 dot11g supported-rate 12 18 24 36 48 54
 dot11g disabled-rate 1 2 5.5 6 9
#
```

(9) 强制指定组播速率

该特性可以强制设置 11g、11a、11n 模式情况下,AP 发送组播或者广播报文使用的发送速率,如图 7-6 所示。一般情况下组播和广播报文采用 AP、STA 协商的最低速率发送,通过该功能可以调整组播报文的发送速率,改善整个 WLAN 网络的性能,并在一定程度上提高组播应用的效果,特别是在进行组播测试时,可以按环境情况,强制组播报文以一个较高的调制速率发送。

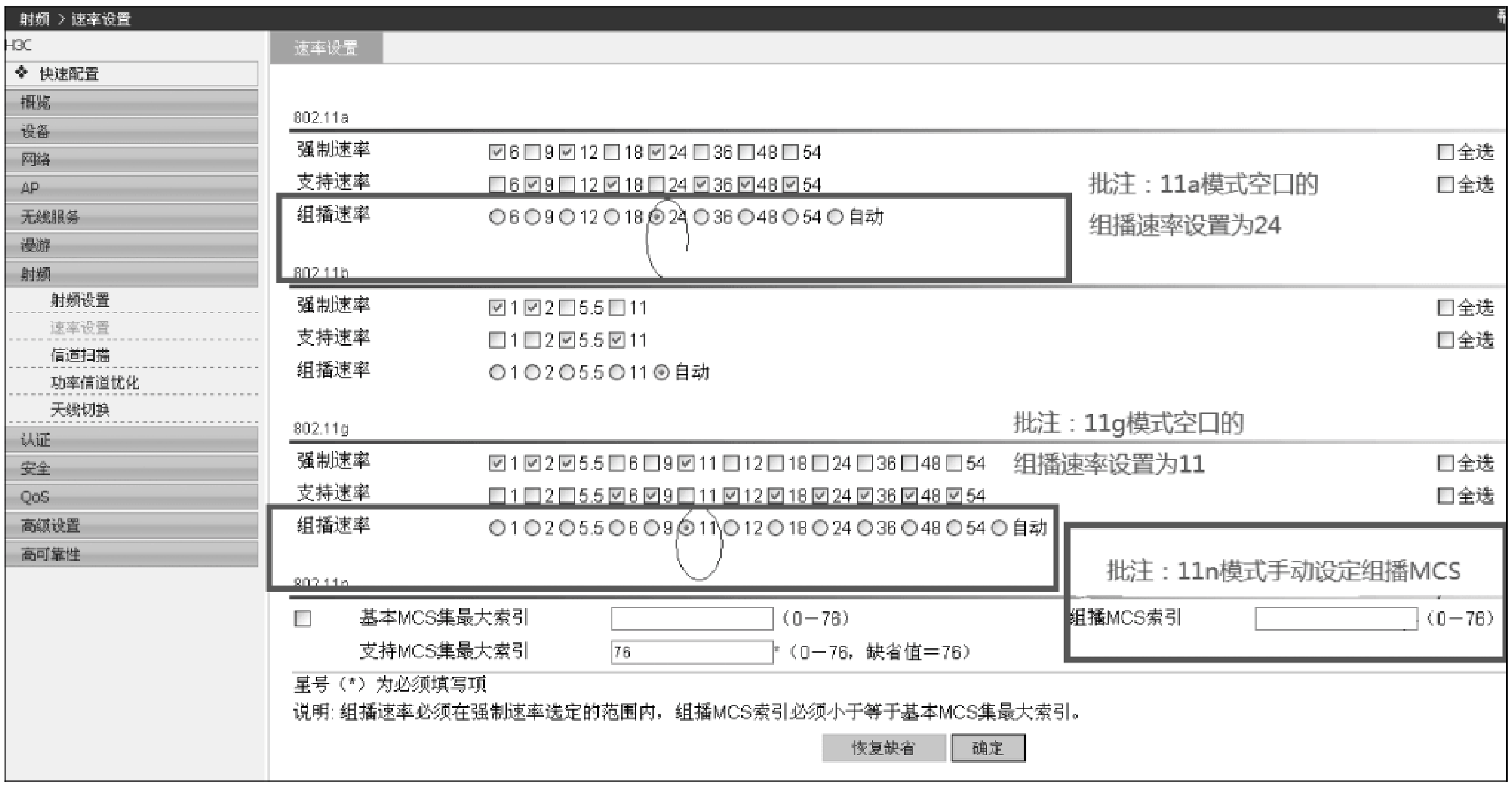


图 7-6　组播速率设置

（10）减小 Beacon 发送间隔

组播数据是在 Beacon 帧后传送的，减小 Beacon 发送间隔有利于减少组播发送时延。同时，该操作也能降低节电模式下无线客户端的休眠时间，提升使用效果。

```
<AC>display current-configuration
#
wlan radio-policy 1
 beacon-interval 60
#
wlan ap ap model WA2620 id 1
 serial-id 219801A0D1C123023703
 radio 1
 radio 2
  service-template 2
  radio-policy 1
  radio enable
#
```

（11）组播丢包优化

组播数据在无线侧发送时没有 ACK 以及重传机制，报文丢失后没有补救措施。为了解决组播丢包问题，可以开启组播优化功能，使得 AP 向客户端发送组播报文时，将组播数据转为单播发送，借用单播 ACK 重传机制，降低丢帧风险。但使用组播转单播发送后，业务数据会在无线侧被发送多次（给多个客户端），可能造成空口利用率升高，请权衡使用。

```
<AC>display current-configuration
#
wlan service-template 3 crypto
 ssid H3C-roam
 bind WLAN-ESS 3
 cipher-suite ccmp
 security-ie rsn
 multicast optimization enable
 service-template enable
#
```

无线AC PSK认证故障排查

余 晨



07 无线产品 > 7.1 AC > 7.1.7 无线 AC PSK 认证故障排查 > 步骤详解

1. 开始

PSK(Pre-Shared Key,预共享密钥)认证需要有无线客户端和设备端配置相同的预共享密钥,如果密钥相同,PSK 接入认证成功;如果密钥不同,PSK 接入认证失败。

2. 流程图相关操作说明

(1) 连接 SSID 是否弹出密码输入框

若正确配置了 PSK 认证,终端连接 SSID 会弹出密码输入框,图 7-7 和图 7-8 所示分别为 Windows 7 和 IOS 的终端密钥输入页面。



图 7-7 Windows 7 的终端密钥输入页面



图 7-8 IOS 的终端密钥输入页面

(2) 检查 PSK 配置

检查全局端口安全是否开启,终端关联 SSID 对应 ESS 接口的 PSK 配置:端口安全模式为 PSK、使能 11key 类型的密钥协商功能并设置密钥。

```
[AC]display current-configuration
#
port-security enable                //全局使能端口安全
#
wlan service-template 1 crypto      //服务模板下 SSID 与 ESS 接口对应
 ssid 123
 bind WLAN-ESS 1
 cipher-suite tkip
 security-ie rsn
 service-template enable
#
#
```

```
interface WLAN-ESS1
 port access vlan 2
 port-security port-mode psk              //使能端口安全模式为 PSK
 port-security tx-key-type 11key          //使能 11key 类型的密钥协商功能
 port-security preshared-key pass-phrase cipher $c$3$SHcJ950t8GUuMW7zb96l75T9lwDNjtFzbJ43
  //设置密钥
#
```

(3) 测试明文关联

创建一个非业务 VLAN 的明文测试 SSID,检查明文关联是否有问题,可参考《无线终端关联失败故障排查云图》。

(4) 密钥是否一致

PSK 接入用户必须使用设备上预先配置的静态密钥,即 PSK(Pre-Shared Key,预共享密钥)与设备进行协商,协商成功后可访问端口;终端在密钥输入页面输入密钥后,若提示密钥不正确,则无法接入无线服务,图 7-9、图 7-10 所示分别为 Windows 7 和 IOS 的终端密钥输入错误显示。

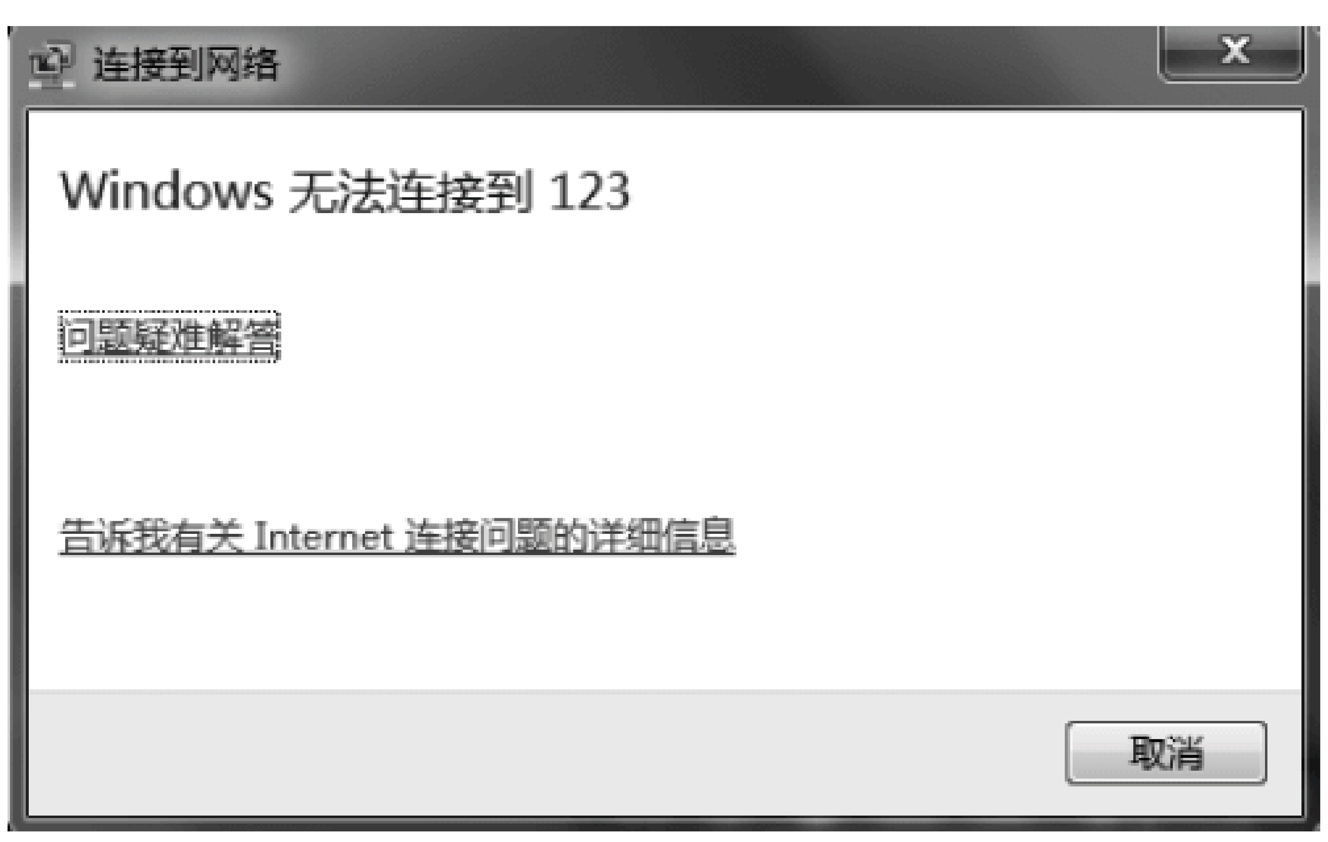


图 7-9 Windows 7 的终端密钥输入错误显示



图 7-10 IOS 的终端密钥输入错误显示

(5) 重置密钥

重新配置预共享密钥如下。

```
[AC-WLAN-ESS2]port-security preshared-key ?
 pass-phrase   Specify port preshare phrase key     //以字符串方式设置预共享密钥
 raw-key       Specify port preshare raw key        //以十六进制方式设置预共享密钥
[AC-WLAN-ESS2]port-security preshared-key pass-phrase 12345678
```

cipher:以密文方式设置密钥。

simple:以明文方式设置密钥。

以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。设置的明文密钥或密文密钥，区分大小写。明文密钥为8～63个字符的字符串或者长度为64位的合法十六进制数；密文密钥为8～117个字符的字符串。不指定cipher或simple时，表示以明文方式设置共享密钥。

(6) 收集diag、debugging信息

收集AC诊断信息和debugging信息。

说明：开启debug之前，请检查CPU和内存的使用情况，确保开启debug不会影响设备的正常运行。收集完信息后请及时关闭debug。

① 当AC在线用户数少于或等于3000时，建议用下面的命令收集信息并使用调试开关进行调试，尽量避免Console口和无线登录AC，信息可能会打印不全，优选有线Telnet。

命令：*debugging wlan mac all*

debugging port-security all

debugging dot1xall

terminal monitor

terminal debugging

② 当AC在线用户数超过3000时，建议等业务闲时关联用户数下降到3000以下，再执行上述操作，收集完信息后请关闭debug。


AC Portal热备故障排查
李晨光
表示上一步结果正常
表示上一步结果出现问题
开始
Portal热备建立
排查client与主备AC间Portal认证情况
排查AC建立1:1热备情况
排查DHBK状态
检查主备AC上的vrrp配置
参考云图 无线AC CAPWAP备份故障排查
检查业务VLAN接口的Portal认证与备份组配置
检查nas-ip和device-id配置
收集debug信息、详细配置信息
拨打热线
400-810-0504
寻求帮助

1. 开始

无线 AC Portal 热备份即无线终端进行 Portal 认证通过后，当主 AC Down 掉后，Client 切到备份 AC 后，Client 用户无须再次进行 Portal 认证，仍然可以访问外部网络。

定位思路是：首先排查故障发生的主备 AC 的 Portal 认证情况，然后排查主备 AC 建立 1+1 热备份情况，再根据具体情况排查配置细节。另外，设备上的 debug 调试信息是重要的定位手段。

2. 流程图相关操作说明

(1) Portal 热备建立

无线 AC Portal 热备建立可以通过命令进行查看 Portal 用户是否建立热备份。

命令：*display portal user all*

例如：通过命令查看 Portal 认证用户信息，可以看到用户名和终端 MAC 地址。

```
<AC-Master>display portal user all
Index:3
 State:ONLINE
 SubState:NONE
 ACL:NONE
Work-mode: primary
  MAC                    IP                  Vlan    Interface
 ---------------------------------------------------------------------
 000d-88f8-0eac          21.1.1.3            2001       Vlan-interface10
 Total 1 user(s) matched, 1 listed.

<AC-Backup>display portal user all
Index:2
 State:ONLINE
 SubState:NONE
 ACL:NONE
 Work-mode: secondary
  MAC                    IP                  Vlan    Interface
 ---------------------------------------------------------------------
 000d-88f8-0eac          21.1.1.3            2001       Vlan-interface10
 Total 1 user(s) matched, 1 listed.
```

(2) 排查 Client 与主备 AC 间 Portal 认证情况

无线 AC Portal 热备首先需要保证 Client 分别与主 AC 和备 AC 之间的 Portal 认证正常，如果不正常，请参考云图《无线 Portal 认证故障排查》。

(3) 排查 AC 建立 1+1 热备情况

无线 AC Portal 热备建立需要建立 AC 间的 1+1 热备，如果主备 AC 间无法建立 1+1 热备，请参考云图《无线 AC CAPWAP 备份故障排查》。

命令：*display hot-backup state*

```
[AC-Master]display hot-backup state
Vlan ID                  : 20
Domain ID                : 1
Link State               : Connect
Peer Board MAC           : 80f6-2ece-4cf8
Peer Board State         : Normal
Hello Interval           : 2000

[AC-Backup]display hot-backup state
Vlan ID                  : 20
Domain ID                : 1
Link State               : Connect
Peer Board MAC           : 80f6-2ece-4cc8
Peer Board State         : Normal
Hello Interval           : 2000
```

(4) 排查 DHBK 状态

无线 AC Portal 热备备份的信息主要为 Client 的 MAC+IP 信息，如果在发生主 AC Down 后，备 AC 需要保证 IP 地址和主 AC IP 地址一致，如果不一致请检查配置。

```
<AC-Master>display current-configuration
#
dhbk enable backup-type symmetric-path
dhbk vlan300
#

<AC-Backup>display current-configuration
#
dhbk enable backup-type symmetric-path
dhbk vlan300
#
```

(5) 检查主备 AC 上的 VRRP 配置

用户的网关在 AC 上，需要检查网关建立 VRRP 的情况与 AP 管理 VLAN 的 VRRP 情况。

```
<AC-Master>display current-configuration
#
    interface Vlan-interface2001        //用户业务 vlan
     ip address21.1.1.1 255.255.255.0
     vrrp vrid 2 virtual-ip 21.1.1.254
     vrrp vrid 2 priority 200
#
#
    interface Vlan-interface2002        //AP 管理 vlan
     ip address 192.168.207.1 255.255.255.0
     vrrp vrid 1 virtual-ip 192.168.207.254
     vrrp vrid 1 priority 200
#

<AC-Backup>display current-configuration
#
    interface Vlan-interface2001
```

```
     ip address21.1.1.2 255.255.255.0
     vrrp vrid 2 virtual-ip 21.1.1.254
 #
 #

     interface Vlan-interface2002
      ip address 192.168.207.2 255.255.255.0
      vrrp vrid 1 virtual-ip 192.168.207.254
 #
```

（6）检查业务 VLAN 接口的 Portal 认证与备份组配置

无线 AC Portal 热备认证需要保证主备 AC 上无线业务 VLAN 上认证与备份配置保持同步，这样才能保证 Portal 热备同步。

```
<AC-Master>display current-configuration
#
interface Vlan-interface2001
  portal server portal method direct
  portal domain portal
  portal backup-group 1
  portal nas-ip 192.168.207.161
#
<AC-Backup>display current-configuration
#
interface Vlan-interface2001
  portal server portal method direct
  portal domain portal
  portal backup-group 1
  portal nas-ip 192.168.207.161
#
```

（7）检查 NAS-IP 和 Device-ID 配置

检查主备 AC NAS-IP 与 Device-ID 配置。

```
<AC-Master>display current-configuration
#
nas device-id 1
radius nas-ip 192.168.202.16
#
<AC-Backup>display current-configuration
#
nas device-id2
radius nas-ip 192.168.202.16
#
```

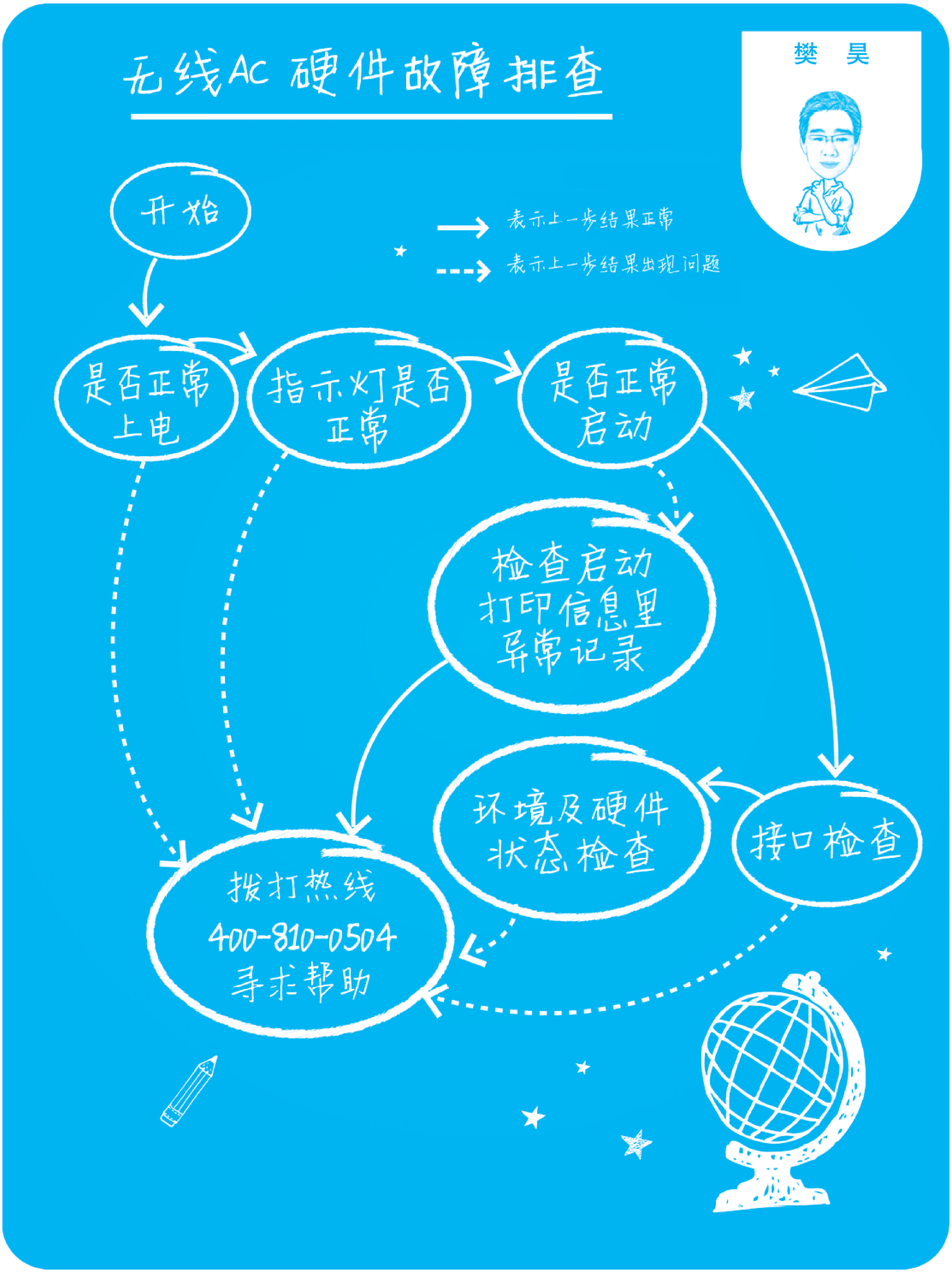
（8）收集 debug 信息、详细配置信息

如果上述步骤仍无法最终解决问题，可以抓取设备侧详细的 debug 信息辅助定位。开启 debug 前检查下 CPU 内存情况，反馈二线确认风险后实施。收集完成后及时关闭。

建议，在业务低峰期抓 debug。业务高峰期可能会有大量其他调试或者日志信息输出，导致有效故障信息打印丢失。

命令：

```
<AC-Master> debugging portal packet interface xxx
<AC-Master> debugging portal tcp-cheat
<AC-Master> debugging portal acl interface xxx
<AC-Master> debugging radius packet
<AC-Backup> debugging portal packet interface xxx
<AC-Backup> debugging portal tcp-cheat
<AC-Backup> debugging portal acl interface xxx
<AC-Backup> debugging radius packet
```


无线AC硬件故障排查
樊 昊
开始
表示上一步结果正常
表示上一步结果出现问题
是否正常上电
指示灯是否正常
是否正常启动
检查启动打印信息里异常记录
环境及硬件状态检查
接口检查
拨打热线
400-810-0504
寻求帮助

1. 开始

无线 AC 硬件故障排查，首先观察能否正常上电，其次观察指示灯是否正常，然后登录查看是否正常启动，最后通过命令行排查端口及设备状态。

2. 流程图相关操作说明

(1) 是否正常上电

观察无线控制器是否正常上电，电源及电源线是否正常。

一般情况下，在满足设备供电环境(电压等)下，如出现无线控制器无法正常上电，在排查接口松动等外在因素后，保持原供电环境并使用新电源线进行替换测试，即可确认故障。

若无线控制器为 AC 板卡，可以使用备用机框进行替换测试，可以排查是否是机框问题导致无法正常上电。

(2) 指示灯是否正常

观察面板呼吸灯和接口指示灯状态，面板呼吸灯和接口指示灯状态说明请参考各型号 AC 的安装指导，确认设备加电后，指示灯未正常亮起则多为硬件故障，指示灯状态可以协助判断当前 AC 工作状态，若故障需要进一步定位。

(3) 是否正常启动

一般设备开机或运行过程重启，常见为下面两种情况。

① 找不到启动文件或启动文件异常，确认启动文件本身是否正常或 Flash 故障导致启动文件异常，此时可以使用 Ctrl+F 组合键格式化 Flash 后重新加载启动文件，如格式化过程报错，需要更换 AC。

② BootWare 提示 CRC 错误：使用 Ctrl+T 组合键在设备开始启动时测试，如出现内存 Fail 则内存故障，需要更换 AC。

如果是控制器框式设备，除上述情况外若主控无法正常启动，需要检查下面两种情况。

① 同一设备两块主控板要求为同样型号，如不一致，需要更换解决。

② 同一设备两块主控板要求使用同样版本，否则会反复启动。

若业务板开机或运行中重启需要检查如下情况。

① 使用 Display Logbuffer 查看单板是否有类似的启动记录，如 Logbuffer 中有对应槽位单板的加载记录，请将业务板更换到其他能正常启动业务板槽位看能否正常启动，如能正常启动一般为主控或机框异常，如果更换槽位后依然没有启动记录，业务板故障可能性最大。

```
%May  3 13:27:17:086 2013 H3C DEVM/4/BOARD_LOADING: Board is loading file on Chassis 1
Slot 7.
%May  3 13:27:17:647 2013 H3C DEVM/5/LOAD_FINISHED: Board has finished loading file on
Chassis 1
```

② 如果双主控设备，可以通过主备倒换确认是否业务板在同一槽位的工作状况确认是否是主控板问题，主备倒换后如业务板卡注册正常，则主控板故障可能最大。

③ 如果同一槽位更换过主控，业务板卡，并且更换的板卡也确认无问题，可以确认为机框问题，需要更换机框解决。

(4) 检查启动打印信息里异常记录

设备上电后，Console 接口打印启动信息是否存在异常。在确认 AC 启动异常后，在许可的操作范围内，先尝试进行“三板斧”(重启、格式化、重新导版本)操作，如果故障依旧可参照本文举例问题处理，若无法找到相对应的信息，请收集相关信息并拨打 800 寻求帮助。

设备如果启动过程中打印如下信息(仅串口能打印)：设备管理框架初始化失败一般为存储标志区的存储器件故障。

```
Driver platform initialize error! Error code:0x%xxxxxxxx
```

(5) 环境及硬件状态检查

① 环境状况检查。各传感器温度应处于低温告警门限与一般级高温告警门限之间，如出现异常温度告警，比如－10 度、255 度等，如果出现超出门限值则一般是温度传感器硬件故障，需要更换 AC。

说明： WX3000 系列不支持此命令。

```
<H3C>display environment
 System Temperature information (degree centigrade):
---------------------------------------------------
 SlotNo     Temperature       Lower limit      Upper limit
 1          255                0                  90
```

② 风扇状况检查。正常应该是 Normal，出现 Fault 一般为故障。

```
<AC>display fan
 Fan    1 State: Normal
 Fan    2 State: Normal
 Fan    3 State: Fault
```

③ 电源状况检查。正常应该是 Normal，出现 Fault 或双电源未显示完全一般为故障。

```
<AC>display power
 Power    1 State: Fault
```

④ 设备运行状况。正常应该是 Normal，出现 Fault 一般为故障。

```
<AC>display device
Slot No     Board Type        Status     Max Ports
0           WX3010ELSW        Normal        -
1           WX3010ERPU        Fault         2
```

(6) 接口检查

设备运行后，检查接口的状态如有异常，一般可以通过端口自检、POE 检查、光口自检排查出大部分的问题。

① 端口自检。检查端口协商链路双工类型：如显示某个端口状态为 half，需要确认是否两端配置不一致导致。

```
<AC>display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

```
Interface            Link Protocol Main IP        Description
NULL0                Up   Up(s)    --
Vlan1                Up   Up       192.168.1.254
Vlan2                Up   Up       --

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
BAGG1                Up   2G(a)   F(a)   T    1
GE1/0/1              Up   1G      F      T    1
GE1/0/2              Up   1G      F      T    1
WLAN-ESS10           Up   --      --     A    2
WLAN-DBSS10:0        Up   --      --     A    2
```

检查端口流控状态：查看配置，是否开启 Flow Control 配置，如果该端口不需要开启则使用 Undo Flow Control 关闭该端口的流控。

```
<H3C>display current-configuration interface
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 flow-control
```

检查端口收发错误报文状态：查看端口是否有大量的错误报文，若排除下面两种状况外一般为硬件问题。

(a) 检查线路质量，检查中间连接的光电转换器。

(b) 两端配置是否一致？是否一端为强制而对端为协商？

```
<H3C>display interface
 GigabitEthernet1/0/2 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 80f6-2e96-f0b2
 Description: GigabitEthernet1/0/2 Interface
 Loopback is not set
 Media type is twisted pair, promiscuous mode set
 1000Mbps-speed mode, full-duplex mode
 Link speed type is force link, link duplex type is force link
 Flow-control is not enabled
 The Maximum Frame Length is 4096
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 Allow jumbo frame to pass
 PVID: 1
 Port link-type: trunk
  VLAN passing: 1(default vlan), 2
  VLAN permitted: 1(default vlan), 2-4094
  Trunk port encapsulation: IEEE 802.1q
 Port priority: 0
 Last clearing of counters:  Never
 Last 300 seconds input:  0 packets/sec 48 bytes/sec 0%
 Last 300 seconds output:  0 packets/sec 28 bytes/sec 0%
```

检查端口 Up/Down 状态：如发现端口频繁 Up/Down，若排查下面几种情况外，一般为硬件问题。

(a) 检查线路和中间连接的光电转换器。

(b) 千兆端口检查光功率是否处于临界值。

(c) 检查两端配置是否一致。

```
<AC>display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 57
```

② POE 检查。检查 POE 功能状态：如设备本身是支持 POE 的设备但却提示"POE is not supported on the port"则说明 POE 硬件存在问题，可尝试采用冷重启的方式重新复位看能否恢复，如不能恢复则可判断为 POE 硬件故障。

```
[SW-GigabitEthernet1/0/1]display this
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 poe enable
#
Return
[SW]interface GigabitEthernet 1/0/1
[SW-GigabitEthernet1/0/1]poe enable
```

③ 光口自检。H3C 设备与其他厂商设备互连，建议光口速率和双工设置要完全一致。使用 display current interface 和 display interface 检查光口状态，光口是否有 CRC 错误？是否在增长？检查光功率是否处于临界值？可以先通过更换光模块、更换尾纤或清洗光模块连接器的方式解决。如未能解决可以将信息及 Diag 搜集后反馈 800 或二线。


无线AC静态路由故障排查
陈 铮
表示上一步结果正常
表示上一步结果出现问题
开始
查看全局路由表中是否有该静态路由
检查出接口状态
查看是否绑定BFD或NQA
检查下一跳地址可达性
检查BFD或NQA配置与状态
检查本静态路由掩码长度
拨打热线
400-810-0504
寻求帮助

1. 开始

静态路由是一种无线设备上常见的路由协议，由管理员手工配置。当网络发生故障或者拓扑发生变化后，静态路由不能自动适应网络，必须由网络管理员手工修改配置。

静态路由是否能够加入到全局路由表中并成功指导报文正确转发，取决于其出接口状态与下一跳可达性，在高端无线控制器上还涉及检测联动的状态等方面。因此无线控制器静态路由定位故障的思路是：首先查看全局路由表中是否存在该静态路由；然后据此相应地检查出接口状态、下一跳地址可达性、BFD 或 NQA 配置、路由优先级等。

2. 流程图相关操作说明

(1) 查看全局路由表中是否有该静态路由

无线控制器上查看全局路由表中是否存在该静态路由。

命令：*display ip routing-table xxx.xxx.xxx.xxx*(目的 IP 网段)

例如：通过上述命令查看，可以确认全局路由表中存在该静态路由。

```
<H3C>display ip routing-table 192.168.2.0
Routing Tables: Public
            Destinations : 1         Routes : 1
Destination/Mask     Proto   Pre   Cost          NextHop          Interface
192.168.2.0/24       Static  60    0             192.168.1.2      GE0/0
```

(2) 检查出接口状态

查看静态路由对应的出接口状态是否正常，正常情况下该接口的物理层状态、协议层状态均为 Up。

命令：*display interface brief*

例如：通过上述命令查看，可以确认出接口的物理层和协议层状态均正常。

```
<H3C>display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down;Stby - standby
Protocol: (s) - spoofing
Interface            Link    Protocol  Main IP          Description
Eth6/0               Down    Down      --
GE0/0                Up      Up        192.168.1.1
```

(3) 检查下一跳地址可达性

查看该静态路由下一跳地址并验证其是否可达。

命令：*display ip routing-table protocol static xxx.xxx.xxx.xxx*(目的 IP 网段)

ping xxx.xxx.xxx.xxx(下一跳 IP 地址)

例如：通过上述命令，可以确认静态路由下一跳地址可达。

```
<H3C>display ip routing-table protocol static 192.168.2.0
...
Static Routing TableStatus : <Active>
SummaryCount : 1
```

```
Destination/Mask    Proto   Pre  Cost        NextHop         Interface
192.168.2.0/24      Static  60   0           192.168.1.2     GE0/0

<H3C>ping 192.168.1.2
  PING 192.168.1.2:56   data bytes, press CTRL_C to break
    Reply from 192.168.1.2: bytes=56 Sequence=1ttl=255 time=1 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2ttl=255 time=1 ms
    Reply from 192.168.1.2: bytes=56 Sequence=2ttl=255 time=1 ms
    ...
```

(4) 查看是否绑定 BFD 或 NQA

中高端无线控制器支持 BFD 和 NQA。查看静态路由是否绑定了 BFD 或 NQA，与 BFD 或 NQA 检测进行联动。

命令：*display current-configuration* | *include xxx.xxx.xxx.xxx*(目的 IP 网段)

例如：通过上述命令查看，可以确认静态路由绑定了 BFD 或 NQA。

```
<H3C>display current-configuration | include 192.168.2.0
ip route-static 192.168.2.0 255.255.255.0 GigabitEthernet0/0 192.168.1.2 bfd control-packet

<H3C>display current-configuration | include 192.168.2.0
ip route-static 192.168.2.0 255.255.255.0 192.168.1.2 track 1
```

(5) 检查 BFD 或 NQA 配置与状态

在配置了静态路由与 BFD 或 NQA 联动的情况下，查看相关配置、状态信息是否正确。正常情况下 BFD 的会话状态为 Up；NQA Track 项的状态信息为 Positive。

命令：*display bfd session*

或　*display trackxxx*(静态路由绑定的 Track 号)

例如：通过上述命令查看，可以确认 BFD 或 NQA 状态正常。

```
<H3C>display bfd session
 Total SessionNum: 1              Init Mode: Active
 IPv4 Session Working Under Ctrl Mode:
 LD/RD          SourceAddr       DestAddr        State Holdtime Interface
53/53           192.168.1.1      192.168.2.2     Up    3300ms   GE0/0

<H3C>display track 1
Track ID: 1
Status: Positive(notify 13 seconds later)
Notification delay: Positive 20, Negative 30 (in seconds)
Reference object:
NQA entry: admin test
Reaction: 10
```

(6) 检查本静态路由掩码长度

最长掩码匹配时全局路由表转发的基本原则。检查到目的 IP 网段的报文转发能否匹配静态路由，即检查该静态路由的掩码是否最长。

命令：*display ip routing-table xxx.xxx.xxx.xxx*(目的 IP 网段)

例如：通过上述命令查看，可以确认本静态路由的掩码不是最长。

```
<H3C>display ip routing-table 192.168.2.0
RoutingTable : Public
SummaryCount : 2

Destination/Mask    Proto    Pre   Cost      NextHop          Interface
192.168.2.0/24      Static   60    0         192.168.1.2        GE0/0
192.168.2.0/25      RIP      100   1         192.168.3.2        GE0/1
```


DHCP Server 故障排查
陈 铮
表示上一步结果正常
表示上一步结果出现问题
开始
检查DHCP配置
查看可用地址
查看内部网络
增加可用IP地址数量
拨打热线
400-810-0504
寻求帮助

07 无线产品 7.1 AC 7.1.11 DHCP Server 故障排查 步骤详解

1. 开始

DHCP Server 定位故障的思路是：先查 DHCP 的配置，再查看是否存在可用 IP 地址，然后查看内部网络是否正常。

2. 流程图相关操作说明

(1) 检查 DHCP 配置

查看当前 DHCP Server 配置，主要包括使能 DHCP，地址池配置。

命令：

① 查看 DHCP Server 使能状态

[*H3C*] *display current-configuration*

② 查看 DHCP Server 地址池配置

[*H3C*] *display dhcp server tree all*

例如：通过命令查看，可以确认已使能 DHCP；并配置了 DHCP 地址池 VLAN30，可分配的地址段为 30.30.30.3 30.30.30.30，掩码为 255.255.255.0，网关为 30.30.30.1。

```
<AC>display current-configuration
#
 dhcp enable
[AC]display dhcp server tree all
Global pool:
Pool name: vlan30
 network 30.30.30.0 mask 255.255.255.0
 network ip range 30.30.30.3 30.30.30.30
 PrevSibling node:vlan20
 gateway-list 30.30.30.1
 expired 1 0 0 0

Pool name: vlan10
 network 10.10.10.0 mask 255.255.255.0
 Sibling node:vlan20
 gateway-list 10.10.10.1
 expired 1 0 0 0

Pool name:1
 PrevSibling node:vlan10
 Sibling node:vlan30
 expired 1 0 0 0
```

(2) 查看可用地址

查看 DHCP Server 地址池是否有可用地址。

命令：*display dhcp server free-ip*

例如：通过命令查看，可以确认 30.30.30.5 至 30.30.30.30 地址还未使用。

```
[H3C] display dhcp server free-ip
IP Range from30.30.30.5    to   30.30.30.30
```

(3) 增加可用 IP 地址数量

如 DHCP Server 地址池无可用地址，则可增加 DHCP 地址池的 IP 地址范围，以此增加该 DHCP 地址池的可用地址数量。

命令：*network ip range min-address max-address*

注意：配置的 IP 地址范围必须在指定的可分配网段范围内，否则该地址池无法分配 IP 地址。

network network-address [*mask-length* | *mask mask*]

例如：通过命令查看，可以确认增加的 IP 网段 30.30.30.3 至 30.30.30.70 地址还未使用。

```
<H3C> system-view
[H3C] dhcp server ip-pool 0 extended
[H3C-dhcp-pool-0] network ip range 30.30.30.3 30.30.30.70      //地址池范围由 30.30.30.3 至 30.30.30.30 增大为 30.30.30.3 至 30.30.30.70
```

(4) 查看内部网络

如内部网络不存在 DHCP 中继，则可参考如下方法排查。

确认 PC 与 DHCP 服务器之间是否可达。

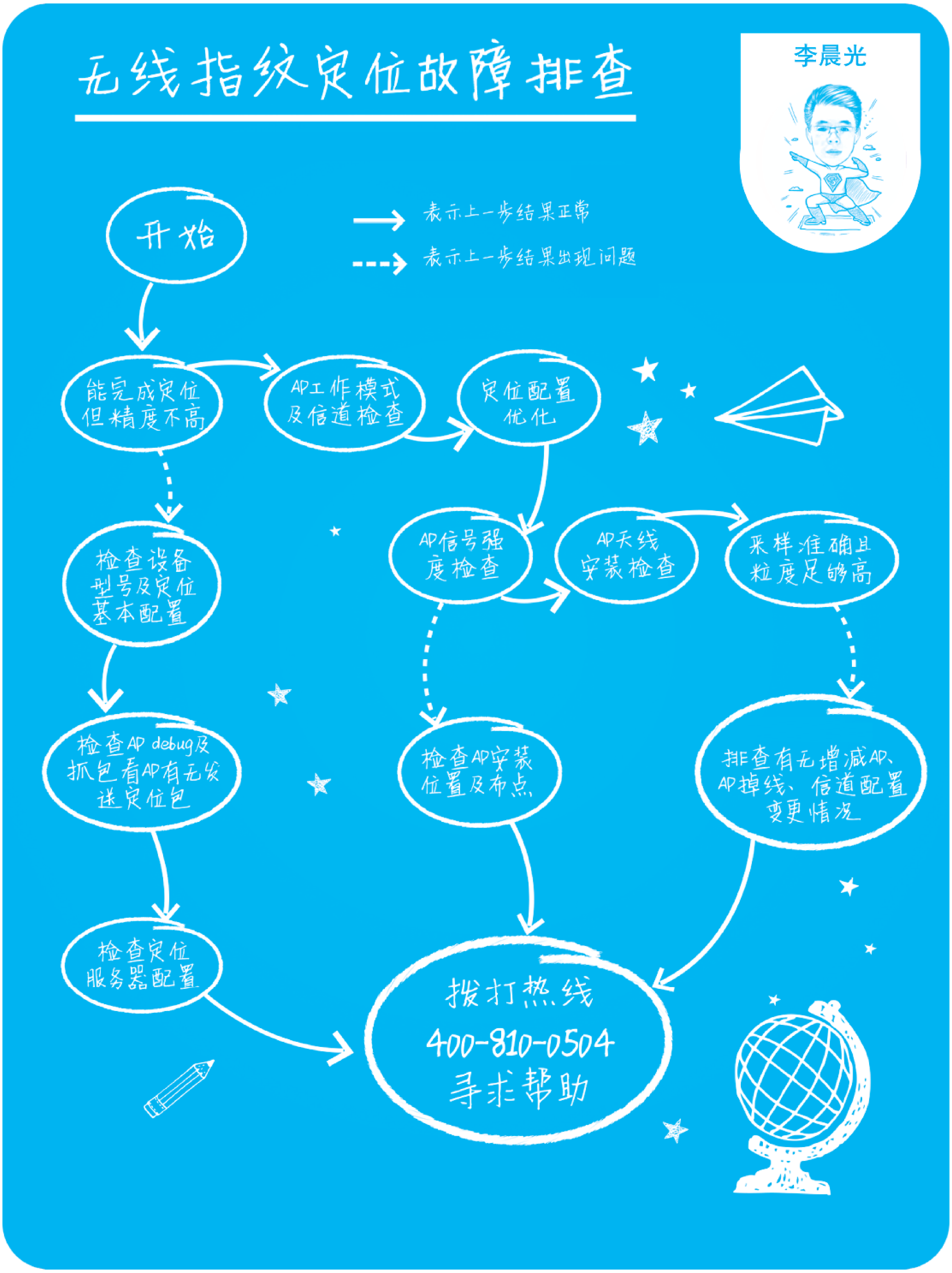
PC 配置一个与 DHCP 服务器同网段的 IP 地址(注意不要和其他地址冲突)，然后使用 PC 来 ping DHCP 服务器，确认是否能够 ping 通。

如内部网络存在 DHCP 中继，则可参考如下方法排查。

① 确认 DHCP 中继与 PC 互连接口的 IP 地址是否与 DHCP 服务器的地址池网段匹配。

② 确认 DHCP 中继与 DHCP 服务器之间是否可达。

分别在 DHCP 中继上 ping DHCP 服务器、DHCP 服务器上 ping DHCP 中继，确认是否存在 ping 不通或者单通的现象。


无线指纹定位故障排查
李晨光
表示上一步结果正常
表示上一步结果出现问题
开始
能完成定位但精度不高
AP工作模式及信道检查
定位配置优化
检查设备型号及定位基本配置
AP信号强度检查
AP天线安装检查
采样准确且粒度足够高
检查AP debug及抓包看AP有无发送定位包
检查AP安装位置及布点
排查有无增减AP、AP掉线、信道配置变更情况
检查定位服务器配置
拨打热线
400-810-0504
寻求帮助

1. 开始

基于 WLAN 的无线定位有多种技术实现途径，有基于信号传播模型的 RSSI 三角定位、RSSI 指纹定位以及 H3C 私有的基于 RTT 光传输时延的三角定位(丘比特)。本云图专门针对 RSSI 指纹定位的故障排查和处理。为保证定位精度能到 10m 左右，无线 RSSI 指纹定位对 AP 部署、天线选型、信号强度都有有别于普通 Wi-Fi 部署的要求。在定位这类故障时，先检查确认 AP 能正确发送定位报文；其次就是检查 AP 部署情况(包括 AP 部署高度、密度、信号强度、天线)是否满足提高定位精度的要求；最后需保证采样的准确性，采样的准确性对定位精度的影响非常大。采样完成后，网络的信道、部署、物理环境不能发生变更，否则需要重新采样。

2. 流程图相关操作说明

(1) 能完成定位但精度不高

首先要确认故障的类别，是完全无法生成定位信息还是仅仅是定位精度不够高？比如误差普遍在 20m 以上或更高。两类故障的定位思路完全不同：对于完全无法生成定位信息的情况，就需要排查 AC 的定位基础配置、AP 型号是否支持定位，以及定位服务器配置是否准确。

(2) 检查设备型号及定位基本配置

① 支持无线定位的设备情况(截至 2015 年 3 月)。只有瘦 AP 支持无线指纹定位。在 B109D023 及之后的版本能支持通用定位协议和 AeroScout 协议(“协议”是指 AP 与服务器通信的报文格式规范，有第三方的 AeroScout 规范和我司私有的规范两种)。支持指纹定位的 AC 和 AP 列举如表 7-3 所示。

表 7-3 支持指纹定位的 AC 和 AP

支持无线指纹定位的 AC	WX3000E、WX5004、WX6000 系列及插卡、WX5500E、WX3500E
支持无线指纹定位的 AP	所有使用 wa2600_fit.bin、wa2600a_fit.bin、wa3600_fit.bin、wa4600_fit.bin 的 AP (支持 11ac 的 AP 需把 radio 模式切换到 11a)，不建议使用 X 分 AP 做定位

② 无线定位的两种方式(区别在服务器是自动发现还是手工配置服务器 IP)。

静态定位方式(推荐)：手工配置定位引擎服务器的 IP 地址，AP 主动向定位服务器发送定位报文，通用定位协议和 AeroScout 协议都支持静态定位方式。

动态定位方式：定位服务器由 AP 去自动发现，需要保证 AP 与定位服务器二层互通，只有 AeroScout 协议支持动态定位方式。

③ 无线指纹定位的基础配置(在不同定位方式下有不同的配置)。

通用定位协议+静态定位方式。

```
<AC> system-view
[AC] wlan rfid-tracking engine-type general
[AC] wlan rfid-tracking enable
[AC] wlan ap ap01 model WA2620E
[AC-wlan-ap-ap01] rfid-tracking engine-addressX.X.X.X
[AC-wlan-ap-ap01] quit
```

AeroScout 协议＋静态定位方式。

```
<AC> system-view
[AC] wlan rfid-tracking enable
[AC] wlan ap ap01 model WA2620E
[AC-wlan-ap-ap01] rfid-tracking engine-addressX.X.X.X
[AC-wlan-ap-ap01] quit
```

AeroScout 协议＋动态定位方式。

```
<AC> system-view
[AC] wlan rfid-tracking engine-detection dynamic
[AC] wlan rfid-tracking enable
[AC] wlan ap ap01 model WA2620E
[AC-wlan-ap-ap01] radio 1
[AC-wlan-ap-ap01-radio-1] rfid-tracking mode all
[AC-wlan-ap-ap01-radio-1] quit
[AC-wlan-ap-ap01] radio 2
[AC-wlan-ap-ap01-radio-2] rfid-tracking mode all
[AC-wlan-ap-ap01-radio-2] quit
[AC-wlan-ap-ap01] quit
```

(3) 检查 AP debug 及抓包看 AP 有无发送定位包

通过远程登录到 AP 上抓取定位 debug 信息，如果能抓到相关 debug，说明 AP 能正常发送定位包。

命令：*debugging wlan as-location all*

telminal debugging

telminal monitor

```
* Mar  4 17:21:00:991 2015 f2-a01-i-1 WASL/7/EVENT :
Client 4cac-0a45-5043 rssi is 47 and nf is 106.
* Mar  4 17:21:00:991 2015 f2-a01-i-1 WASL/7/FRAME : Put MU message into the queue.
* Mar  4 17:21:00:993 2015 f2-a01-i-1 WASL/7/EVENT : Read MU message from queue.
* Mar  4 17:21:00:993 2015 f2-a01-i-1 WASL/7/FRAME : Receive MU message.
* Mar  4 17:21:00:995 2015 f2-a01-i-1 WASL/7/EVENT :WASL begin to send frame to server.
* Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/EVENT :
WASL report ip address is 10.100.56.225.
* Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/EVENT :
WASL report port is 1144.
* Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/VERBOSE : AE message:
00 01 01 26 18 e8 5a 48 00 01 00 01 4c ac 0a 45
50 43 74 25 8a 86 f0 a0 02 00 74 25 8a 86 f0 b0
00 00 0b 00 ba b6 b1 f1 c5 96 00 50 00 21 00 00
00 01 00 d6 50 00 3a 01 18 59 36 78 76 e3 4c ac
0a 45 50 43 4c ac 0a 45 50 43 60 ab 1a 14 d6 de
04 02 00 00 a0 00 21 04 00 08 43 4d 43 43 2d 57
45 42 01 08 82 84 8b 96 0c 12 18 24 03 01 0b 07
06 43 4e 20 01 0d 1e 2a 01 00 32 04 30 48 60 6c
2d 1a 8c 01 1b ff 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 33 1a 8c 01
1b ff 0
* Mar  4 17:21:00:997 2015 f2-a01-i-1 WASL/7/EVENT : WASL send frame to server.
* Mar  4 17:21:00:997 2015 f2-a01-i-1 WASL/7/EVENT :Send message to AE successfully.
```

另外，通过在 AP 上行口抓包也能判断。AP 发送定位报文的目标 IP 地址为定位引擎服务器 IP 地址，端口号 1144。

(4) 检查定位服务器配置

检查定位服务器近期有没有调整过配置，包括是否有 IP 地址变更、定位参数调整等。检查定位服务器到 AP 的网络路由是否可达。

(5) AP 工作模式及信道检查

① AP 工作模式。WLAN 网络在完成定位的同时要兼容 Wi-Fi 终端接入，根据在二者间的工作分配，AP 有不同的工作模式。不同的模式下 AP 在定位扫描和 Wi-Fi 接入的时间分配有区别，需要针对具体情况设置合理的工作模式。AP 工作模式有如下 3 种。

Monitor Mode：AP 按照 1、6、11 信道周期切换的方式扫描周围信道，每个信道停留的时间为 60ms。工作在此模式下的 AP 无法做用户接入。

Access Mode：AP 工作在此模式下可以正常提供 Wi-Fi 用户接入功能，同时还能扫描 AP 当前工作的信道，也即是 AP 只能扫描监控一个信道。

Hybrid Mode：AP 在大部分的时间都工作在一个信道用于提供 Wi-Fi 接入和信道监控，也会留出较短的时间用于扫描非工作信道。工作在该模式下的 AP 对非工作信道的监控定位效果有限。

在实际的定位应用中，一般推荐 monitor 和 access 模式混搭使用，不推荐使用 Hybrid 模式。

命令：*work-mode monintor*

例如：通过命令设置 AP 的工作模式为 monitor。

```
wlan ap f1-a06-o-1 model WA2620i-AGN id 207
 priority level 7
 serial-id 219801A0CNC144000364
 work-mode monitor
 undo broadcast-probe reply
 radio 1
  channel 149
  radio enable
 radio 2
  channel 6
  radio enable
```

② 信道设置。RSSI 指纹定位要求在同一个位置能有尽量多的 AP 能扫描到终端的无线信号。所以在 AP 部署时，同一个区域的 AP 需要采用相同的信道。推荐的方式是一个楼层设置一个信道，不同的楼层设置不同的信道。

楼层与楼层之间的区域比如楼梯、手扶电梯附近可以增加几个 monitor 模式的 AP 完成过渡，monitor AP 可以同时监控上下两个楼层的信道。

(6) 定位配置优化

无线指纹定位建议配置忽略 Beacon 帧(不上报 Beacon 监控信息，降低 AP CPU 开销)以及设置定位报文最低 RSSI 门限值(从无线信号传播模型看，RSSI 越低，距离 AP 越远，信号波动越大，并且当 RSSI 低于 20 后，RSSI 值随距离变化不敏感，基本丧失参照价值，所以需要剔除 RSSI 小于 20 的报文)。

命令：*wlan rfid-tracking ignore beacon*

例如：配置无线定位忽略 Beacon 帧。

命令：*wlan rfid-tracking rssi-threshold 20*

例如：配置无线定位最低 RSSI 门限值为 20。

(7) AP 信号强度检查

什么是 Wi-Fi 指纹，指纹就是许多个 AP 收到的终端信号强度的一个集合，它与终端所处的位置相关。只有当能接收终端信号的 AP 越多，指纹才越丰富精确，才能保证定位的精度。

从经验上看，只有当大多数区域点位都能收到 3 个及以上 AP 的 Beacon 信号，并且强度大于－75dBm 方能保证较好的定位效果。所以定位要求 AP 有一定的部署密度。

(8) 检查 AP 安装位置及布点

当 AP 的部署不满足信号强度的要求时（即大多数区域都能收到 3 个及以上 AP 的 Beacon 信号并且强度大于－75dBm 的要求），就需要考虑是否增加 AP 以及调整 AP 的部署位置。

① 对于层高在 4m 左右的商场，推荐 AP 部署密度在 20m 一个。

② 对于层高超过 4m 的商场，AP 应该部署更密。如果层高超过 6m，定位效果会下降。

③ 对于层高低于 4m 的场景，比如地下车库，一般层高在 3m 以下。AP 部署密度可以相应降低，比如 30m 一个 AP。

还有一些通用规范，如：AP 要均匀部署；不要靠近墙角/障碍物等。

(9) AP 天线安装检查

推荐使用普通全向天线，这类天线的辐射方向图比较稳定，且水平波瓣图接近于圆形，如图 7-11 所示。

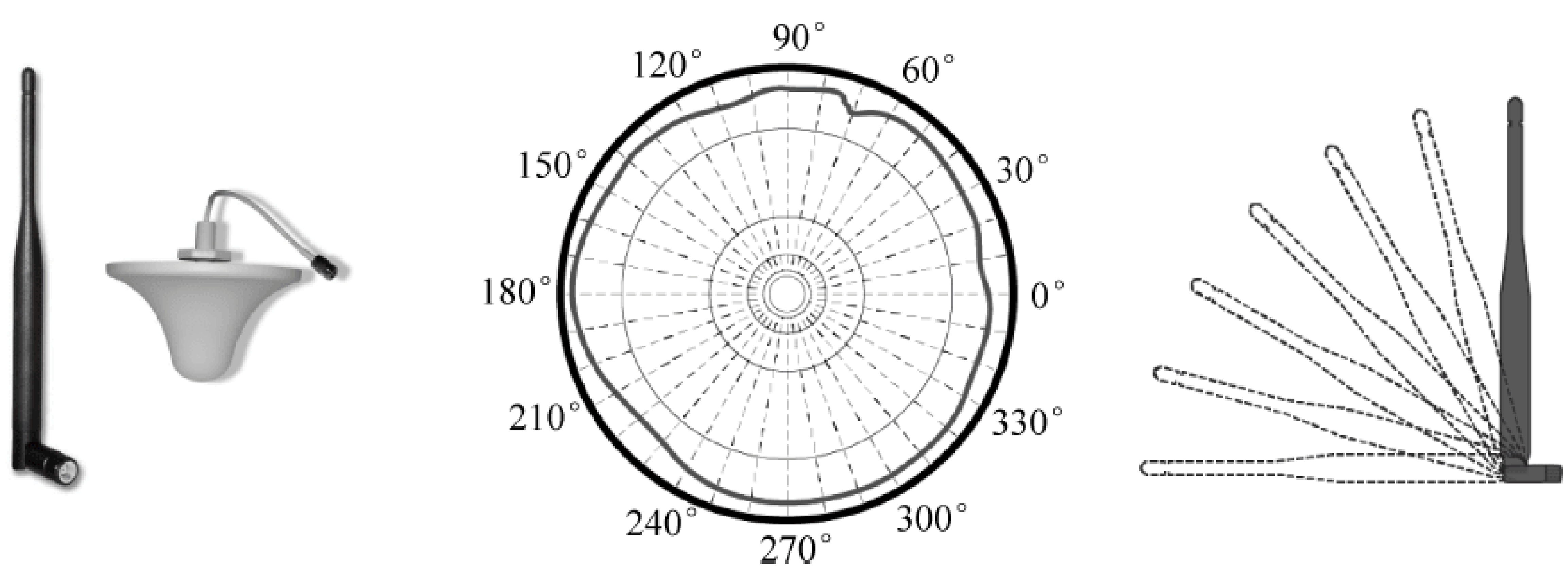


图 7-11　普通全向天线

对于有智能天线的 AP，比如 WA2620i、WA4620i-ACN 等，建议关闭智能天线功能。

命令：*undo smart-antenna enable*

例如：关闭 AP 智能天线。

```
#
wlan ap b1-a01-i-2 model WA4620i-ACN id 102
 priority level 7
 serial-id 210235A1BSC147001281
 undo broadcast-probe reply
 rfid-tracking engine-address 10.100.56.225
```

```
radio 1 type dot11an
 channel 149
 radio-policy 1
 service-template 2 vlan-id 80
 undo smart-antenna enable
 power lock
radio 2
 channel 1
 radio-policy 1
 service-template 2 vlan-id 80
 service-template 4
 undo smart-antenna enable
 power lock
 radio enable
#
```

（10）采样准确且粒度足够高

无线 RSSI 指纹定位需要预先采样，即预先收集各物理位置的 RSSI 指纹，再与目标终端的 Wi-Fi 信号进行匹配从而"估算"终端的位置。所以"采样"信息收集的准确性直接关系到定位的精准度。

采样的过程解析：由测试人员拿着采样 Wi-Fi 终端遍历所有的物理点位，在这个过程中由 AP 收集并由服务器记录终端的信号强度，再结合测试人员在地图上输入的点位坐标，汇总成位置与信号强度的指纹库 $<(x,y)、RSSI_{AP1}、RSSI_{AP2}、\cdots、RSSI_{APn}>$。不同定位引擎服务器在采样方式上的区别主要在于通过何种方式能让工程师在地图上既方便又准确地输入采样坐标。以智慧图为例进行举例说明。

智慧图采样时需要测试人员携带两部手机，包括采样手机和信号源手机。

① 采样手机上运行采样 App，并携带地图，通过 Wi-Fi 网络与定位服务器建立连接。采样时，要求沿采样路线匀速行走，并每隔一段距离单击确认当前所在位置。所有的数据将实时存放在服务器端。

② 信号源手机充当采样的信号源，AP 接收到采样手机的信号并上报到服务器。为了获取更多的样本，要求在短时间内手机发出大量的报文，一般通过安装 Wi-Fi 扫描仪 App 实现。

这种采样方式的最大优势是节省时间，只需要人走一遍就完成信号的采样。相比于采用网格采样、笔记本采样的方式更为高效。

为了达到较高的定位精度，要求采样过程中测试人员移动速度尽量慢（速度不超过 0.3m/s），位置信息确认要足够准确，并且采样线路要覆盖的足够密（任意目标点位为中心，半径 2 米内必须有采样线路能覆盖）。建议同一条线路来回走两遍，用于消除人体信号遮挡造成的采样误差。

（11）排查有无增减 AP、AP 掉线、信道配置变更情况

为保证采样数据的准确性，必须在完成了所有的 AP 部署上线、信道、工作模式参数配置之后再来进行采样操作。

如果在采样完成后发生增加 AP、减少 AP、AP 掉线、AP 信道配置变更或者环境的物理结构发生改变等情况，必须重新进行采样，才能保证定位服务器有准确的指纹数据库，才能准确定位。


赵 杰
VRRP+NQA联动失败故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
NQA收发报文统计是否正常
查看Track状态是否为Positive
查看VRRP状态是否正常
检查Track与VRRP联动绑定关系
检查网络连通性
检查Track与NQA绑定配置
检查VRRP配置是否正确
检查VRRP虚地址与实地址是否一致
检查CPU占用率
检查VRRP主备间二层链路是否正常
检查探测报文发送频率/超时时间
拨打热线
400-810-0504
寻求帮助

1. 开始

定位故障的思路是：首先观察 NQA 收发统计报文是否一致，判断 NQA 检测是否正常。如果 NQA 检测报文收发不一致且差值数量在增长，则检查网络质量、设备 CPU 利用率以及探测报文发送频率/超时时间的设置；如果 NQA 检查报文收发一致或者收发差值没有增长，则需要检查 Track 状态；如果 Track 状态异常，则需要检查 NQA 配置；如果 Track 状态正常，则需要检查 VRRP 状态是否正常；如果 VRRP 状态异常，则需要检查主备之间二层链路是否稳定以及 VRRP 配置是否一致；如果 VRRP 状态正常，则需要检查 Track 与 VRRP 联动配置以及 VRRP 实地址与虚地址是否一致。

2. 流程图相关操作说明

(1) NQA 收发报文统计是否正常

NQA 统计数据记录报文收发数量以及检测失败报文分类统计数量，通过收发报文数量差值可以判断 NQA 检测是否正常，如果多次查看发送报文数量与接收报文数量差值稳定不变，则说明 NQA 探测正常，反之则说明 NQA 探测异常。

命令：*display nqa statistics*

例如：通过命令查看 NQA 报文统计信息，检查发送报文数量和接收数量是否一致，判断 NQA 探测是否正常。

```
[Master]display nqa statistics
 NQA entry (admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 192.168.2.10
      Start time: 2015-04-27 13:05:02.2
      Life time: 1351 seconds
      Send operation times:7045              Receive response times: 6620
      Min/Max/Average round trip time: 1/51/5
      Square-Sum of round trip time: 274288
    Extended results:
      Packet loss in test: 6%
      Failures due to timeout:425
      Failures due to disconnect: 0
    Reaction statistics:
      Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
      2        probe-fail         consecutive        7044            425
```

(2) 检查网络连通性

检查 NQA 探测目的地址是否可达，如果目的 IP 地址 ping 不通，主要检查以下内容。

① 检查接口是否 Up，链路是否故障。

② 检查互连端口统计，检查错误报文统计是否在增长。

③ 检查链路状况是否有震荡，是否有端口频繁 Up/Down。

④ 检查 NQA 目的 IP 地址路由是否可达。

⑤ 端口下是否开启了认证、ACL 过滤等安全功能。

⑥ 如果是光介质，检查光衰减是否在正常范围之内。

(3) 检查 CPU 占用率

一般情况下,CPU 占用率超过 90%时可能会导致探测报文上送 CPU 丢包,这时需要排查 CPU 高的原因。

命令:*display cpu-usage*

例如:查看设备的 CPU 占用率。

```
<Master>display cpu-usage
Slot 1 CPU usage:
      92% in last 5 seconds
      90% in last 1 minute
      81% in last 5 minutes
```

(4) 检查探测报文发送频率/超时时间

根据网络的流量大小、设备的性能、链路质量状况等因素,合理配置探测报文的发送间隔以及失效时间。修改 NQA 探测报文的发送间隔和允许连续的探测失败次数。

命令:*frequency interval*

reactionitem-number checked-element probe-fail threshold-type consecutive

consecutive-occurrences action-type trigger-only

例如:配置 NQA 探测报文发送间隔为 1500ms,最多允许连续 5 个报文失效。

```
[Master-nqa-admin-test-icmp-echo]display this
#
 type icmp-echo
  frequency 1500
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
```

(5) 查看 Track 状态是否为 Positive

通过命令查看 Track 项状态,如果 Track 状态稳定在 Positive,则说明 Track 正常,如果 Track 状态为 Negative 或者 Invalid 状态,则说明 Track 状态异常。

命令:*display tracktrack-entry-number*

例如:通过命令查看 Track 1 的当前状态。

```
[Master]display track 1
Track ID: 1
  Status:Positive
  Duration: 0 days 0 hours 14 minutes 11 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

(6) 检查 Track 与 NQA 绑定配置

配置 Track 项时,如果引用了错误的 NQA 测试组,则该 Track 项的状态为 Invalid。

例如:Track 项错误的引用了 NQA 测试组 admin test Reaction 1 导致 Track 项状态为 Invalid。

```
[Master]display track 1
Track ID: 1
```

```
      Status:Invalid
      Duration: 0 days 0 hours 1 minutes 9 seconds
      Notification delay: Positive 0, Negative 0 (in seconds)
      Reference object:
        NQA entry:admin test
        Reaction:1
    [Master]display nqa reaction counters admin test
      NQA entry (admin admin, tag test) reaction counters:
        Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
        2       probe-fail        consecutive      833           73
```

(7) 查看 VRRP 状态是否正常

通过命令检查主备 VRRP 状态是否正常，如果主设备 VRRP 状态为 Master，备设备 VRRP 状态为 Backup，则 VRRP 状态正常，反之其他状态则 VRRP 状态异常。

命令：*display vrrp interface vlan x*

例如：通过命令查看主备设备 VLAN 1 的 VRRP 状态信息。

```
[Master]display vrrp interface vlan 1
IPv4 Virtual Router Information:
 Running mode: Standard
 Total number of virtual routers on interface Vlan-interface1 : 1
 Interface     VRID   State      Running   Adver    Auth       Virtual
                                  Pri       Timer    Type         IP
 ---------------------------------------------------------------------------
 Vlan1            1   Master      120       100      None       192.168.1.1

[Backup]display vrrp interface  vlan 1
IPv4 Virtual Router Information:
 Running mode: Standard
 Total number of virtual routers on interface Vlan-interface1 : 1
 Interface       VRID   State       Running   Adver    Auth       Virtual
                                     Pri       Timer    Type         IP
 ---------------------------------------------------------------------------
 Vlan1            1      Backup      100       100      None       192.168.1.1
```

(8) 检查 VRRP 配置是否正确

主备的 VRRP 配置保持一致时，VRRP 状态才可以正常，VRRP 关键配置包括 VRID、虚 IP 地址、认证方式以及密钥相同，通过命令检查主备配置是否正常。

命令：*display current-configuration*

例如：使用命令查看检查主备的 VRRP 配置是否一致。

```
[Master]display current-configuration
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 priority reduced 30
#
[Backup]display current-configuration
```

```
#
interface Vlan-interface1
 ip address 192.168.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 100
#
```

(9) 检查 VRRP 主备间二层链路是否正常

VRRP 协议通过二层报文相互建立连接,当 VRRP 协议报文转发 VLAN 二层不通时,将影响主备之间的 VRRP 状态,如果 VRRP 协议报文转发 VLAN 二层不通,请检查如下几项。

① 检查接口是否 Up,链路是否故障。

② 检查链路状况是否有震荡,是否有端口频繁 Up/Down。

③ 端口下是否开启了认证、ACL 过滤等安全功能。

④ 如果是光介质,检查光衰减是否在正常范围之内。

(10) 检查 Track 与 VRRP 联动绑定关系

如果 Track 状态发生变化,则无法与应用模块联动,检查需要关联的 Track 项是否已创建,或与应用模块关联的 Track 项是否正确。

例如:查看配置的 VRRP 是否与 Track 项正确关联。

```
[H3C]display current-configuration interface vlan 1
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
vrrp vrid 1 track 1 priority reduced 30
#
return
[H3C]display track 1
Track ID:1
   State: Positive
   Duration: 0 days 1 hours 49 minutes 57 seconds
   Notification delay: Positive 0, Negative 0 (in seconds)
   Tracked object:
     NQA entry: admin test
     Reaction: 1
```

(11) 检查 VRRP 虚地址与实地址是否一致

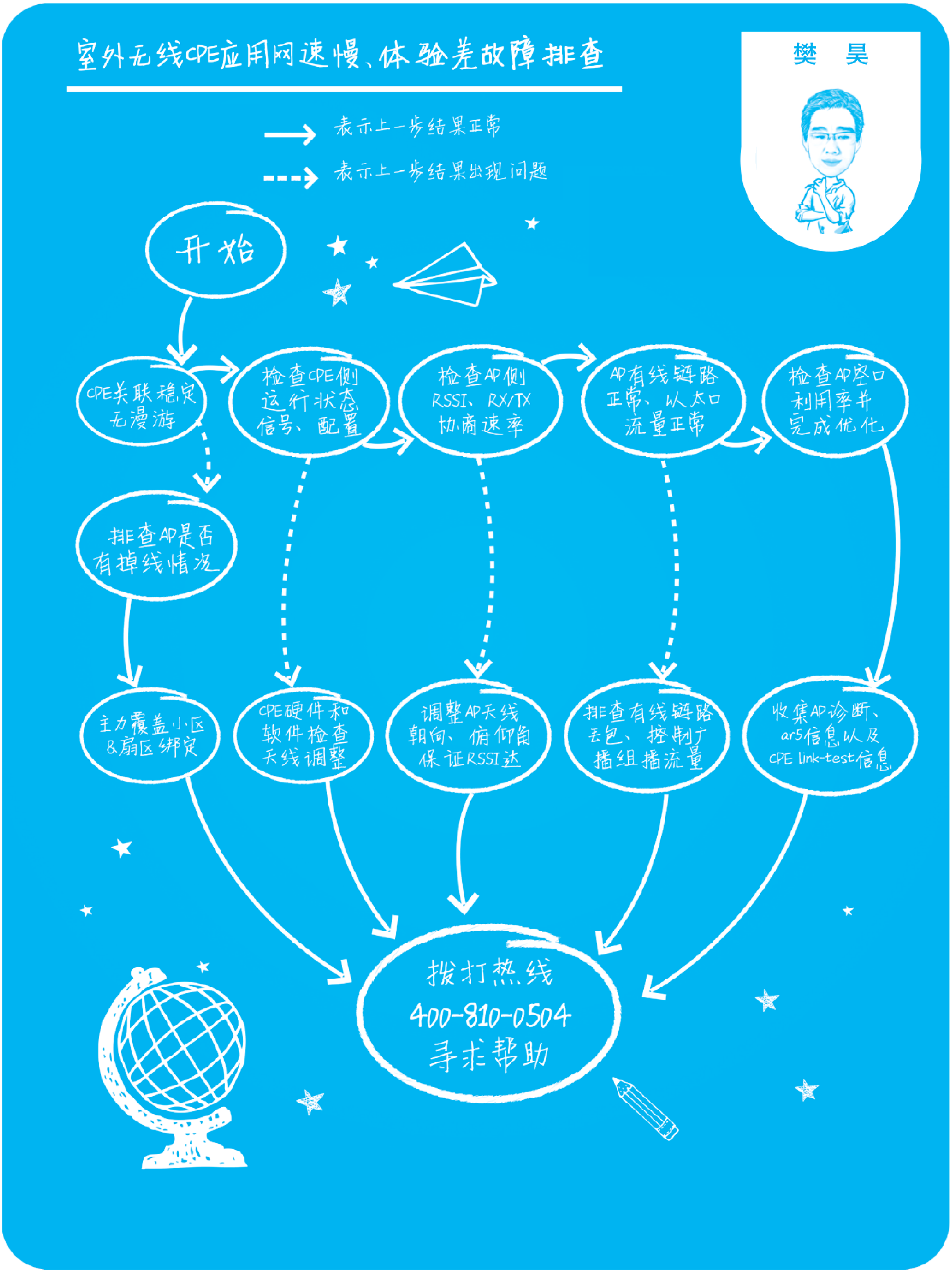
VRRP 正常状态时,设备的 VRRP 虚地址与实地址在同一个网段且不相同,主设备 VRRP 虚地址与实地址相同时,查看主备 VRRP 状态正常,当 NQA 检测到目的地址不可达时,Track 将联动 VRRP 失败,VRRP 状态将不能正常的切换。

命令:*display current-configuration interface vlan x*

例如:使用命令查看 VLAN 接口 VRRP 实地址与虚地址是否相同。

```
[H3C]display current-configuration interface vlan 1
#
interface Vlan-interface1
```

```
ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 priority reduced 30
#
return
```



室外无线CPE应用网速慢、体验差故障排查
樊 昊
表示上一步结果正常
表示上一步结果出现问题
开始
CPE关联稳定无漫游
检查CPE侧运行状态信号、配置
检查AP侧RSSI、RX/TX协商速率
AP有线链路正常、从太口流量正常
检查AP空口利用率并完成优化
排查AP是否有掉线情况
主力覆盖小区&扇区绑定
CPE硬件和软件检查天线调整
调整AP天线朝向、俯仰角保证RSSI达
排查有线链路丢包、控制广播组播流量
收集AP诊断、ar5信息以及CPE link-test信息
拨打热线
400-810-0504
寻求帮助

1. 开始

WLAN＋CPE 在农村宽带无线中应用较为普遍。由于 CPE 大多分布在山区等有线网络覆盖不到的地区，受山地地形和长距离信号传输的衰耗等因素的影响，室外无线 CPE 经常会出现上网速度慢、看视频卡顿等体验类问题。当出现这类问题后，远程定位的思路是先明确故障发生的范围，是单个 CPE 还是某一个扇区下的很多 CPE，或者故障扩散到整个基站塔及回传网络。如果故障范围锁定在单个 CPE 或者 AP，定位时可以从"点"和"面"两个切入点着手："点"是指该 CPE 的信号强度、RSSI、协商速率以及 link-test 重传丢帧情况；"面"是指整个 AP 的大环境，如空口利用率、关联用户数、有线端口流量等。两方面综合考虑，方能快速准确的定位问题。

2. 流程图相关操作说明

(1) CPE 关联稳定、无漫游

室外 WLAN 应用中，AP 安装于 2G/3G 基站或高塔上，信号覆盖范围广。CPE 侧经常能收到多个 AP 发送过来的信号，从而导致 CPE 可能在多个 AP 间发生漫游，漫游过程中的丢包和延时可能导致网络不稳定。在 WLAN 实施中应尽量避免 CPE 频繁漫游情况的发生(比如可以采用不同的扇区用不同 SSID 的方式，保证 CPE 的准确接入)。

命令：*display wlan client roam-track mac-address xxxx-xxxx-xxxx*

例如：查看 MAC 地址 70ba-ef0a-9c8d 的 CPE 是否发生过漫游，以及漫游发生的时间。

```
<H3C>display wlan client roam-track mac-address 70ba-ef0a-9c8d
                        Roam Track Table
--------------------------------------------------------------------------
 BSSID            Online-time(d:h:m:s)  AC-IP-address
--------------------------------------------------------------------------
 5866-ba61-fcd0 0000:23:56:20           -HOME AC-
 5866-ba99-db00 0000:00:54:31           -HOME AC-
 5866-ba61-fcd0 0000:01:53:20           -HOME AC-
--------------------------------------------------------------------------
```

(2) 排查 AP 是否有掉线情况

当 CPE 关联的 AP 发生掉线时，也可能导致 CPE 失去主覆盖小区，在其他扇区的 AP 间频繁漫游。

命令：*display wlan ap connection record mac-address xxxx-xxxx-xxxx*

例如：查看 MAC 地址 c4ca-d9f3-aa60 的 AP 是否发生过掉线，根据记录的上线时间来判断 AP 是否掉线过。

```
<AC>display wlan ap connection record mac-address c4ca-d9f3-aa60
 MAC Address     Serial ID                   State     Time
--------------------------------------------------------------------------
 c4ca-d9f3-aa60  210235A0RXC11C003173        Run       2015-03-04 00:04:27
 7425-8a90-4860  219801A0LVC142000326        Offline   2015-02-13 11:06:04
```

(3) 主力覆盖小区和扇区绑定

CPE 发生频繁漫游,可能是缺少主力覆盖小区导致,即多个 AP 在该区域的信号强度都差不多,CPE 在这些 AP 间发生来回漫游。可以使用 WLAN 信号测试仪(WirelessMon)来测试周边的无线信号。当发现确实有多个 WLAN 信号同时存在且强度差不多时,就要考虑是否需要调整 AP 的覆盖范围,包括移开非主覆盖小区的 AP 天线、调整天线俯仰角等。

(4) 检查 CPE 侧运行状态、信号、配置

以 H3C WB521X 为例,如图 7-12 所示。

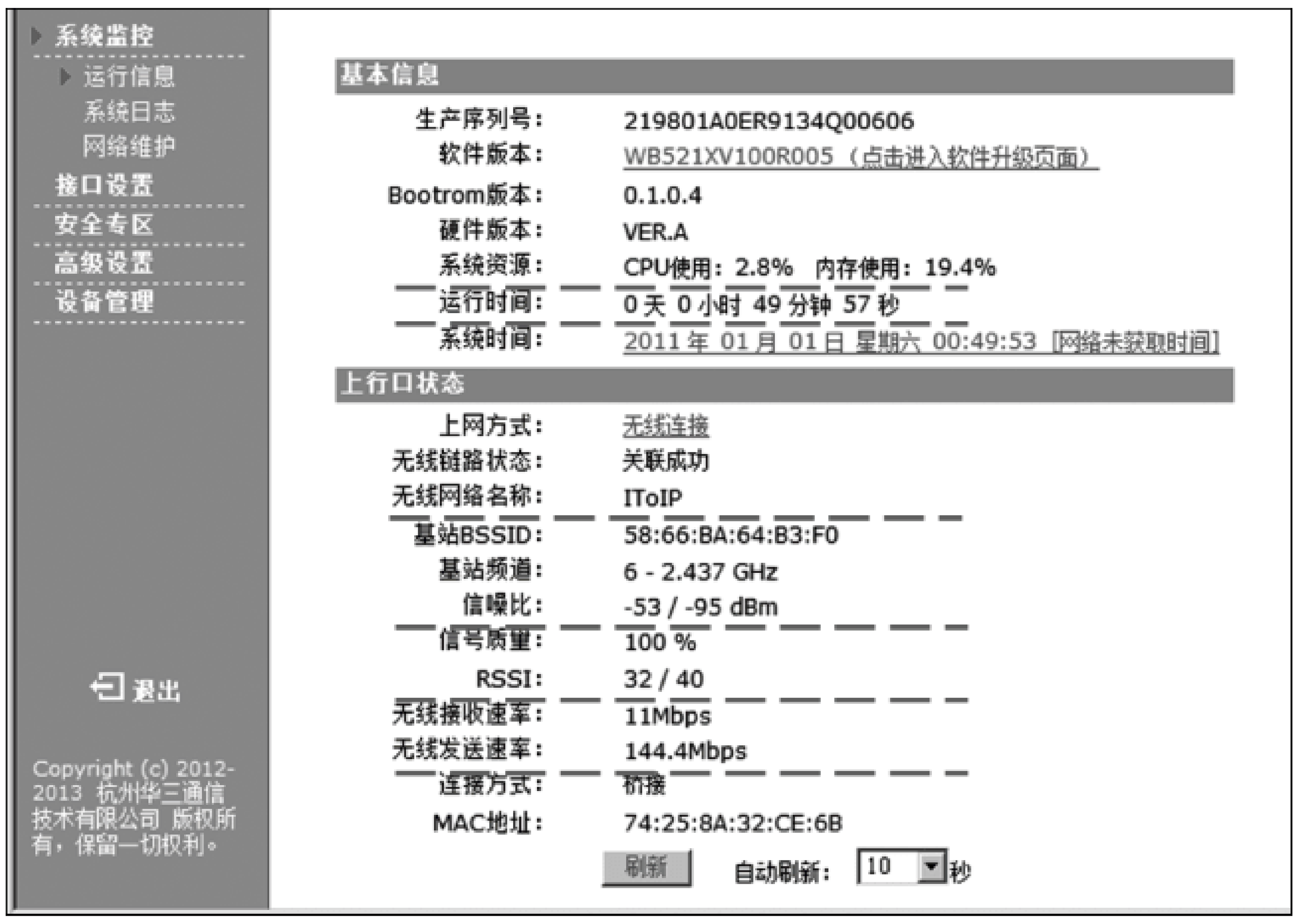


图 7-12　H3C WB521X

CPE 的 CPU 和内存利用率不超过 60%。

CPE 关联无线网络名称正确。

CPE 收到 AP 的信号强度大于 −65dBm,噪声强度小于 −95dBm。

CPE RSSI,值大于 30,双天线差值小于 10。

CPE 接收和发送速率。

(5) CPE 硬件和软件检查、天线调整

检查 CPE 硬件状态,以 H3C WB521X 的安装规范性为例,如表 7-4 所示。

表 7-4　H3C WB521X 的安装规范性

项　目	检　查　项	检 查 内 容
CPE 室外安装	CPE 放置位置	CPE 垂直安装,网卡朝下,螺丝或喉箍牢固固定
	CPE 天线角度	CPE 放置位置与无线基站不超过 2km,无遮挡
	CPE 防水	网线处做好防水弯,卡紧下盖或拧紧防水接头
网线布放	网线长度	选择质量较好的五类,超五类线材,外皮保护层完整,长度建议越短越好,网线最长不超过 100m
	网线走线	强弱电分开走线,网线单独固定和捆扎,切勿与电线等线缆搭接
	水晶头制作	采用直连线序(T-568B)方式压制水晶头,网口和水晶头卡连接应有清脆的咔哒声
POE 注入器安装	POE 注入器连接	CPE 接 POE 供电模块处需做好防水弯避免雨水进入
	POE 注入器供电	以我司 POE 注入器为例子,供电后,模块灯应常亮
CPE 运行检查	CPE 指示灯	CPE Power 灯常亮、LAN 灯闪烁、Diag 灯常灭
	CPE 信号强度	信号强度指示灯应调整至 2 格以上信号;Web 页面上信噪比应大于 −65dBm,RSSI 大于 30,差值小于 10

如果 CPE 上显示 AP 信号强度小于－70dBm，需要考虑是否调整 CPE 朝向及高度。

如果 CPE 双天线 RSSI 差值太大，需要考虑是否 CPE 或者 AP 天线存在故障，尝试替换测试。

另外 CPE 上需要开启 RTS/CTS 保护，防止上行方向由于 CPE 间隐藏节点形成冲突导致性能下降(H3C WB521X 默认开启 RTS/CTS)。

(6) 检查 AP 侧 RSSI、RX/TX 协商速率

在 AP 侧查看 CPE 信号强度，RSSI 应该大于 30。RX/TX 协商速率越高越好(至少不低于 11Mbps)。

命令：*display wlan client mac-address xxxx-xxxx-xxxx verbose*

例如：查看 CPE 信号强度。

```
<AC>display wlan client mac-address 5cdd-70b7-88b1 verbose
 Total Number of Clients                    : 1
                                   Client Information
 ----------------------------------------------------------------------------------
 MAC Address                                : 5cdd-70b7-88b1
 User Name                                  : -NA-
 IP Address                                 : 0.0.0.0
 AID                                        : 20
 AP Name                                    : zd-hedian-ap-1
 Radio Id                                   : 2
 Antenna Id                                 : 0
 Service Template Number                    : 97
 SSID                                       : sz-hedian-1
 BSSID                                      : 7425-8a8f-3190
 Port                                       : WLAN-DBSS97:8733
 VLAN                                       : 1001
 State                                      : Running
 Power Save Mode                            : Active
 Wireless Mode                              : 11gn
 Channel Band-width                         : 20MHz
 SM Power Save Enable                       : Disabled
 Short GI for 20MHz                         : Supported
 Short GI for 40MHz                         : Not Supported
 STBC TX capability                         : Supported
 STBC RX capability                         : Supported
 Support MCS Set                            : 0,1,2,3,4,5,6,7,8,9,
                                                10,11,12,13,14,15
 BLOCK ACK-TID 0                            : BOTH
 QoS Mode                                   : WMM
 Listen Interval (Beacon Interval)          : 1
 RSSI                                       : 30
 Rx/Tx Rate                                 : 65/144.4
 Client Type                                : PRE-RSNA
 Authentication Method                      : Open System
 Authentication Mode                        : Central
 AKM Method                                 : None
 4-Way Handshake State                      : -NA-
 Group Key State                            : -NA-
 Encryption Cipher                          : Clear
 Roam Status                                : Normal
```

```
Roam Count                            : 0
 Up Time (hh:mm:ss)                   : 9 Days, 02:55:07
 Serial Number                        : 219801A0KP913CQ01701
 Device Information                   : WB521X-E
 Software Version                     : WB521X-EV100R001
 Associated AP RSSI                   : -NA-
 Associated AP SNR                    : -NA-
 Tx Power (dBm)                       : -NA-
 Rx Packets                           : 0
 Rx Bytes                             : 0
 Tx Packets                           : 0
 Tx Bytes                             : 0
 Tx Dropped Packets                   : 0
 Command Execution Result             : -NA-
--------------------------------------------------------------------------------
```

RSSI 值应该在 30 以上为良好，不能低于 25，否则需要调整 AP 位置或者天线角度来提升信号强度。

RX/TX 速率：65 以上为优，低于 24 为较差。

另外，对于 11n 的 AP 和 CPE 配合，需保证每根天线接收到的信号强度 RSSI 都相差不大，差值不能超过 10，否则可能会影响 MIMO 效果。在 AP 隐藏模式下通过如下命令查看 11n 多根天线的 RSSI。

命令：*display ar5drv 2 client all rssi*

例如：查看 WA2620X MIMO 共 2 根天线的 RSSI 情况。

```
[AP-hidecmd]display ar5drv 2 client all rssi
Station table info : Table(0x858e7744) Num(22/128)
Hash info :
H0(1) H1(1) H2(2) H3(2) H4(2) H5(1) H6(2) H7(2)
H8(2) H9(1) H10(1) H11(1) H12(1) H13(1) H14(1) H15(1)
--------------------------------------------------------------------------------
        Station AID(1) Hash(1) Mac(70ba-ef8a-fa17) Used(YES) Ht:(YES)
[Station Current Rssi Info]:
 [Rate    RateFlag   Aver   Ctl0   Ctl1   Ctl2   Ext0   Ext1   Ext2  ]
 [6.5     H-L-2-S    0      0      0      0      0      0      0     ]
 [13.0    H-L-2-S    47     42     45     0      0      0      0     ]
 [19.5    H-L-2-S    47     42     45     0      0      0      0     ]
 [26.0    H-L-2-S    48     43     46     0      0      0      0     ]
 [39.0    H-L-2-S    48     44     46     0      0      0      0     ]
 [52.0    H-L-2-S    46     41     44     0      0      0      0     ]
 [58.5    H-L-2-S    0      0      0      0      0      0      0     ]
 [65.0    H-L-2-S    47     42     45     0      0      0      0     ]
 [72.2    H-S-2-S    0      0      0      0      0      0      0     ]
 [78.0    H-L-2-D    47     41     45     0      0      0      0     ]
 [104.0   H-L-2-D    46     42     45     0      0      0      0     ]
 [117.0   H-L-2-D    47     42     45     0      0      0      0     ]
 [130.0   H-L-2-D    46     41     45     0      0      0      0     ]
 [144.4   H-S-2-D    47     43     45     0      0      0      0     ]
--------------------------------------------------------------------------------
```

(7) 调整 AP 天线朝向、俯仰角保证 RSSI 达标

通过天线方位和俯仰角的调整来保障天线主波瓣覆盖 CPE 所在区域，提升 RSSI 信号强度，如图 7-13 所示。

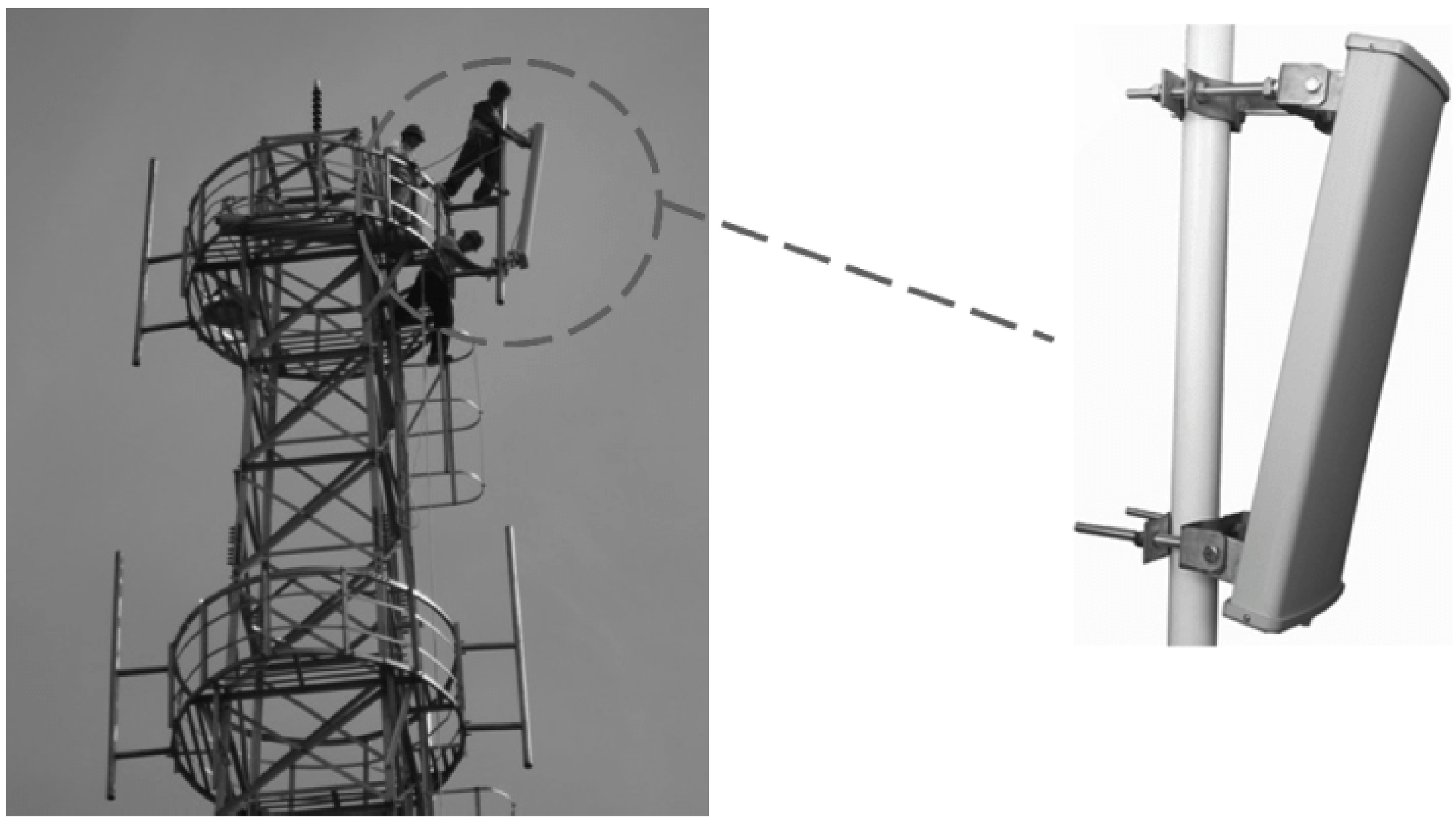


图 7-13 调整 AP 天线朝向、俯仰角

另外，为保证 11n 多天线 RSSI 值均衡，要注意天线的极化连接方向，即天线的多根“辫子”中至少有一个水平极化 ANT 和一个垂直极化 ANT 分别连接 AP 的两个“TR”射频口（“TR”，即能完成无线信号的发和收；“R”只能完成信号的接收，不能向外发送信号）。WA2620X-AGNP 和 WA2620X 图例说明如图 7-14、图 7-15 所示。

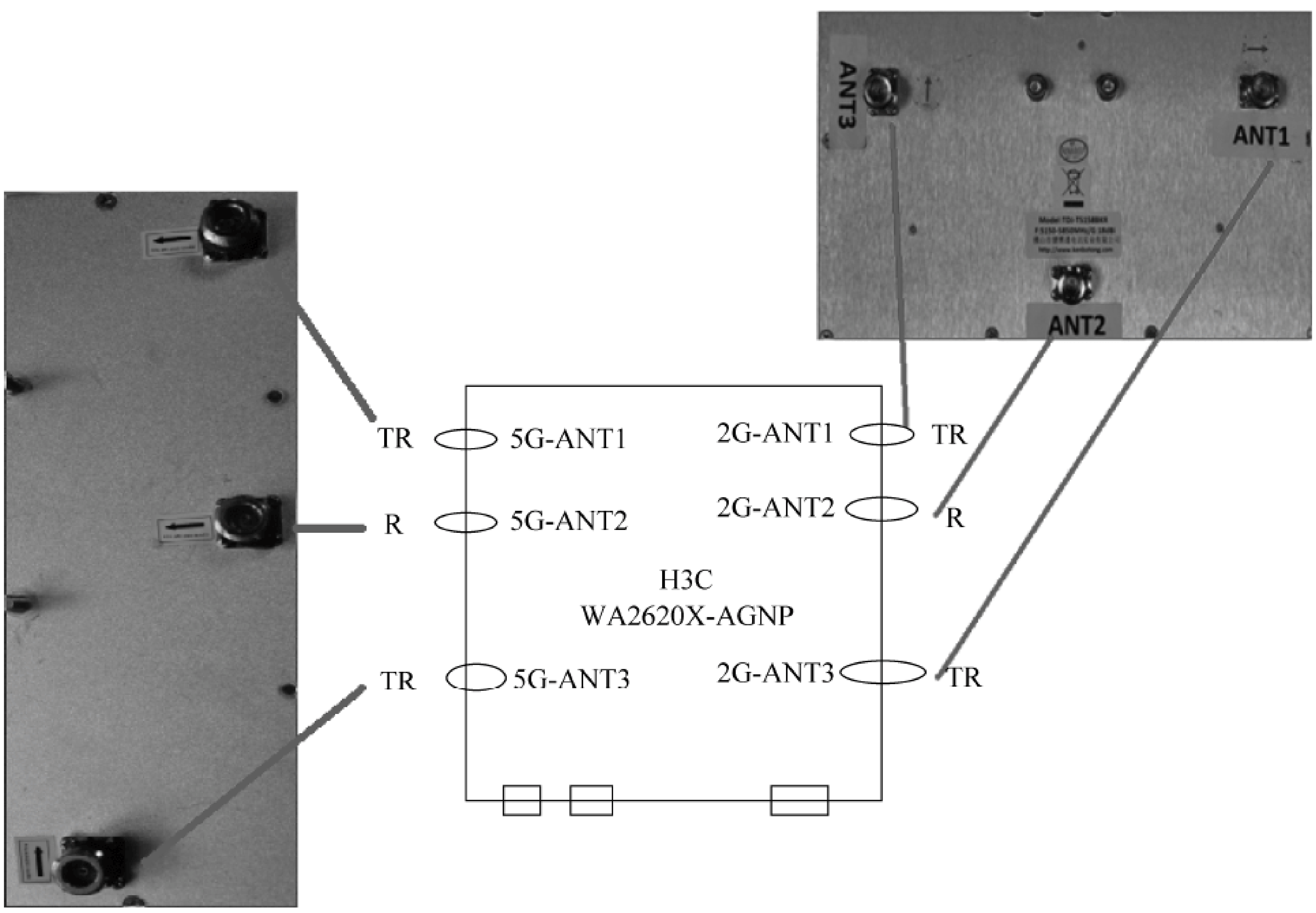


图 7-14 WA2620X-AGNP 天线的极化连接方向

(8) AP 有线链路正常、以太口流量正常

如果无线业务走集中转发，需要检查 AP 到 AC 链路是否丢包和延迟抖动。如果无线业

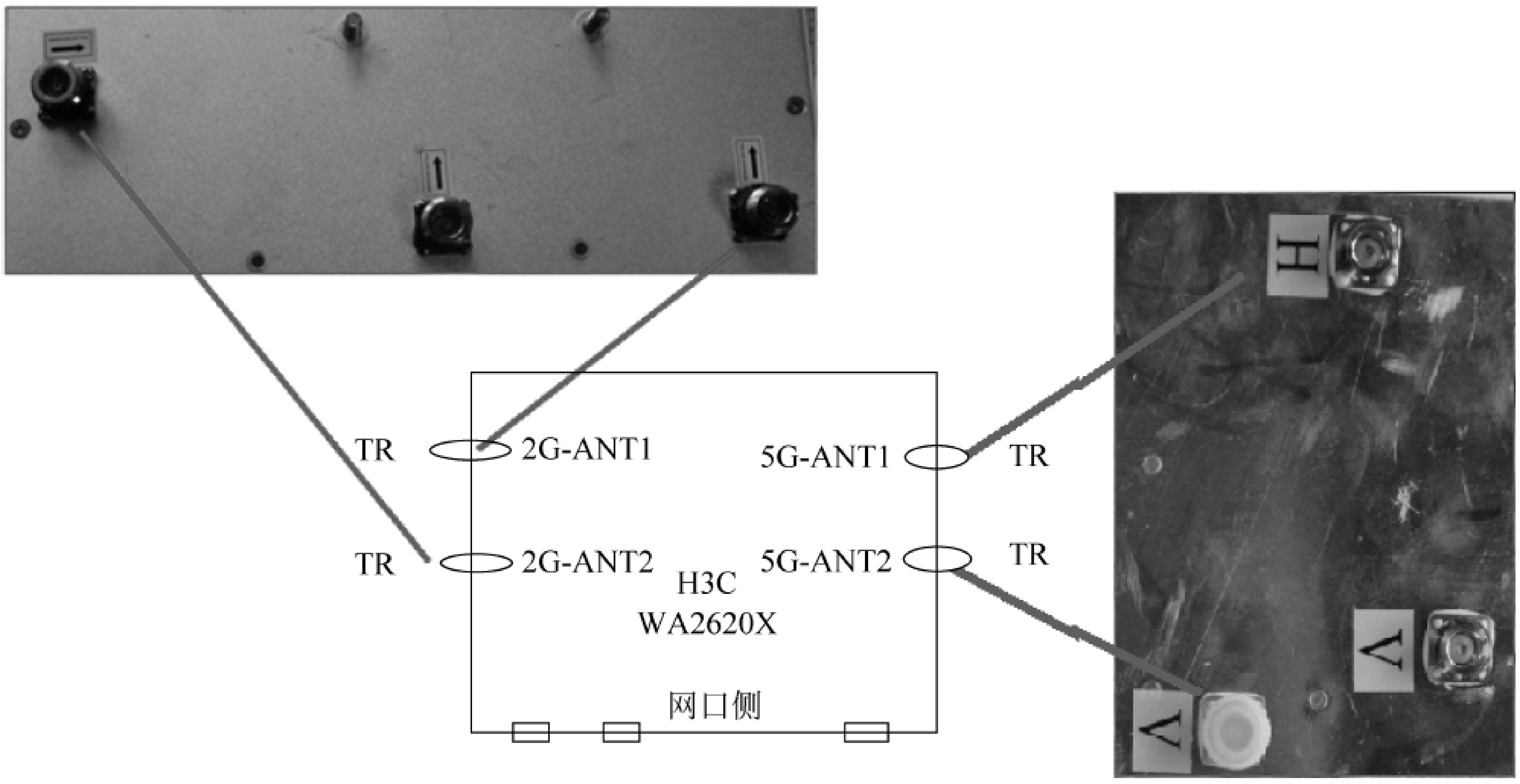


图 7-15 WA2620X 天线的极化连接方向

务走本地转发，比如走 BAS 通过 PPPoE 拨号上网，就需要检查 AP 到 BAS 的有线链路是否有丢包和延迟抖动(可以在 AP 上创建三层业务 VLAN 接口，配置 IP 地址测试链路)。

命令：*ping -s 1472 -f x.x.x.x*

例如：ping 1472 字节包(MTU 1500)，强制不分片，检测 AP 到 BAS 链路是否丢包。

```
<AC>ping -s 1472 -f 117.130.195.46
  PING 117.130.195.46: 1472  data bytes, press CTRL_C to break
    Reply from 117.130.195.46: bytes=1472 Sequence=1 ttl=21 time=20 ms
    Reply from 117.130.195.46: bytes=1472 Sequence=2 ttl=21 time=20 ms
    Reply from 117.130.195.46: bytes=1472 Sequence=3 ttl=21 time=20 ms
    Reply from 117.130.195.46: bytes=1472 Sequence=4 ttl=21 time=20 ms
```

另外，还需要关注下 AP 有线口流量：如果流量较大，比如超过 15Mbps，说明无线业务整体基本可用，但无线链路可能存在拥塞，部分 CPE 体验可能较差，建议降低单 CPE 限速门限阈值；如果流量非常小，比如上下行共不到 5Mbps，说明业务受阻比较严重，这就需要进一步排查链路瓶颈在有线还是无线侧。

命令：*display interface*

例如：查看 AP 以太口上下行流量。

```
<AP>display interface
 GigabitEthernet1/0/1 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: c4ca-d99b-88e0
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair, promiscuous mode set
 100Mbps-speed mode, full-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 The Maximum Frame Length is 1600
 PVID: 1
 Port link-type: trunk
```

```
   VLAN passing: 1(default vlan), 1004
   VLAN permitted: 1(default vlan), 2-4094
   Trunk port encapsulation: IEEE 802.1q
  Port priority: 0
  Last clearing of counters:   Never
  Last 300 seconds input:341 packets/sec 478806 bytes/sec 4%
  Last 300 seconds output:236 packets/sec 21657 bytes/sec 0%
  Input (total):  3050778893 packets, 3307536728112 bytes
          3048227174 unicasts, 2048133 broadcasts, 503586 multicasts, - pauses
  Input (normal):  3050778893 packets, 3307536728112 bytes
          3048227174 unicasts, 2048133 broadcasts, 503586 multicasts, - pauses
  Input:  0 input errors, 0 runts, 0 giants, - throttles
          0 CRC, 0 frame, 0 overruns, 0 aborts
          0 ignored, - parity errors
  Output (total): 2618635823 packets, 680308489268 bytes
          2616812898 unicasts, 351695 broadcasts, 1467547 multicasts, - pauses
  Output (normal): 2618632140 packets, 680301126430 bytes
          2616812898 unicasts, 351695 broadcasts, 1467547 multicasts, - pauses
  Output: 3683 output errors, 0 underruns, 0 buffer failures
          3683 aborts, 0 deferred, 0 collisions, 0 late collisions
```

(9) 检查有线链路丢包、控制广播组播流量

如果定位到有线链路存在丢包和较大的延迟抖动，则需要先排除掉有线网络的故障，比如以太口存在错包、上联交换机丢包等。

还有一种可能情况是有线网络存在环路导致广播风暴引起丢包。可以通过查看有线口广播、组播报文占比来分析定位。如果广播和组播报文占比超过 30%，就需要进一步排查具体原因。

命令：*display interface*

例如：查看 AP 以太口广播、组播报文占比情况。

```
 <AP>display interface
  GigabitEthernet1/0/1 current state: Up
  IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: c4ca-d99b-88e0
  Description: GigabitEthernet1/0/1 Interface
  Loopback is not set
  Media type is twisted pair, promiscuous mode set
  100Mbps-speed mode, full-duplex mode
  Link speed type is autonegotiation, link duplex type is autonegotiation
  The Maximum Frame Length is 1600
  PVID: 1
  Port link-type: trunk
   VLAN passing   : 1(default vlan), 1004
   VLAN permitted: 1(default vlan), 2-4094
   Trunk port encapsulation: IEEE 802.1q
  Port priority: 0
  Last clearing of counters:   Never
  Last 300 secondsinput:   341 packets/sec 478806 bytes/sec 4%
  Last 300 seconds output:   236 packets/sec 21657 bytes/sec 0%
  Input (total):  3050778893 packets, 3307536728112 bytes
```

```
            3048227174 unicasts, 2048133 broadcasts, 503586 multicasts, - pauses
    Input (normal):  3050778893 packets, 3307536728112 bytes
            3048227174 unicasts, 2048133 broadcasts, 503586 multicasts, - pauses
    Input:  0 input errors, 0 runts, 0 giants, - throttles
            0 CRC, 0 frame, 0 overruns, 0 aborts
            0 ignored, - parity errors
    Output (total): 2618635823 packets, 680308489268 bytes
            2616812898 unicasts, 351695 broadcasts, 1467547 multicasts, - pauses
    Output (normal): 2618632140 packets, 680301126430 bytes
            2616812898 unicasts, 351695 broadcasts, 1467547 multicasts, - pauses
    Output: 3683 output errors, 0 underruns, 0 buffer failures
            3683 aborts, 0 deferred, 0 collisions, 0 late collisions
```

(10) 检查 AP 空口利用率并完成优化

查看 AP 空口利用率。

命令：*display ar5drv 2 channelbusy*

例如：查看 radio 2 的空口利用率。

```
[AP-hidecmd]display ar5drv 2 channelbusy
ChannelBusy information
 Ctl Channel:      11      Channel Band: 20M
 Ext Channel:
 Record Interval(s):   9
 Date/Month/Year: 09/03/2015
         Time(h/m/s):    CtlBusy(%) TxBusy(%)   RxBusy(%)   ExtBusy(%)
 01        14:14:54         19           1           17            0
 02        14:14:45         20           1           18            0
 03        14:14:36         16           1           14            0
 04        14:14:27         30          14           14            0
 05        14:14:18         20           1           18            0
 06        14:14:09         19           1           16            0
 07        14:14:00         19           1           17            0
 08        14:13:51         20           2           18            0
 09        14:13:42         18           1           16            0
 10        14:13:33         22           1           20            0
 11        14:13:24         22           1           19            0
 12        14:13:15         23           1           20            0
 13        14:13:06         24           3           20            0
 14        14:12:57         20           2           17            0
 15        14:12:47         22           2           19            0
 16        14:12:38         22           3           18            0
 17        14:12:29         19           1           16            0
 18        14:12:20         20           1           18            0
 19        14:12:11         17           1           15            0
 20        14:12:02         19           2           15            0
```

几种常见的故障情况分析及处理建议如下。

① RxBusy→TxBusy，RxBusy＋TxBusy 总和达到 80 以上。例如 RxBusy 平均 80，TxBusy 小于 5。此种情况属于典型的 WLAN 内部干扰，即同频 AP 之间互相可见，竞争一个信道介质，导致空口利用率 RX 方向异常偏高。解决的办法包括合理的信道规划、功率规划、关闭 RRM 低速率、关闭广播 Probe 应答和调大 Beacon 帧间隔、二层隔离等。建议按照《技基通知 2014(005)号——关于下发行业无线优化操作规范的通知》完成网络优化。

② RxBusy 和 TxBusy 相差不多，RxBusy+TxBusy 总和达到 80 以上。例如 RxBusy 平均 50，TxBusy 平均 40 左右。此种情况下一般体验尚可，如果仍有终端上网慢，最有可能的原因是无线 CPE 数量过多，或者部分 CPE 业务量较大，占用了过多带宽。建议开启终端限速或者扩容增加 AP 解决。

③ RxBusy<<TxBusy，RxBusy+TxBusy 总和达到 80 以上。例如 TxBusy 平均 80，RxBusy 小于 5。此种情况说明 AP 下行方向发包受阻。在室外 CPE 应用中较为常见。发生这类故障时，一般伴随着 Client Verbose 信息中 TX 协商速率低，即 AP 发送给 CPE 的帧经常丢失，进而降速重传，最后导致 AP 发送的帧都是低速帧。低速帧会大量消耗空口资源，进而导致 CPE 体验集体变差。

遇到这种情况，可以先观察该 AP 下的 CPE 信号强度，如果 RSSI 都在 30 以上，则可以尝试在 AP 侧通过强制 TX 高速率解决，11n 情况下建议尝试 MCS 13。

命令：*ar5drv 2 fixrate unidata rate-11n MCS 13*

ar5drv 2 fixrate enable

例如：配置 AP 的下行 TX 速率为 MCS 13。

```
[WA2620X-hidecmd]ar5drv 2 fixrate unidata rate-11n MCS 13
[WA2620X-hidecmd]ar5drv 2 fixrate enable
```

在 20M 频谱带宽、2 条空间流的情况下，MCS 与物理速率的对应关系如表 7-5 所示。

表 7-5　MCS parameters for optional 20MHz，$N_{SS}=2$，$N_{ES}=1$，EQM

MCS Index	Modulation	R	$N_{BPSCS}(i_{SS})$	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data rate(Mbps)	
								800ns GI	400ns GI(see NOTE)
8	BPSK	1 * 2	1	52	4	104	52	13.0	14.4
9	QPSK	1/2	2	52	4	208	104	26.0	28.9
10	QPSK	3/4	2	52	4	208	156	39.0	43.3
11	16-QAM	1/2	4	52	4	416	208	52.0	57.8
12	16-QAM	3/4	4	52	4	416	312	78.0	86.7
13	64-QAM	2/3	6	52	4	624	416	104.0	115.6
14	64-QAM	3/4	6	52	4	624	468	117.0	130.0
15	64-QAM	5/6	6	52	4	624	520	130.0	144.4
NOTE—The 400ns GI rate values are rounded to 1 decimal place									

④ 还有一种导致空口体验差的情况是存在非 WLAN 干扰，但非 WLAN 干扰存在的证据不明显。从空口利用率上看，当 CtlBusy 大大超出 RxBusy 和 TxBusy 总和时，可以认为是非 WLAN 干扰存在的一个证据。常见的非 WLAN 干扰源有如无线摄像头、靠得太近的 3G/4G 基站等(室外 AP 要求与 3G/4G 基站天线距离保持在 5m 以上)。

当怀疑存在非 WLAN 干扰时，可以用排除法来证明。即先排除周边的 WLAN 干扰源，比如关闭周边 AP，并使用 omnipeek 抓包发现无法抓取 Wi-Fi 报文。如果此种情况下仍然存在 CtlBusy 异常高，可以作为外部干扰存在的证据。

(11) 收集 AP 诊断、ar5 信息以及 CPE link-test 信息

收集 AP 诊断、CPE link-test 及 CPE client verbose 信息，联系 400 热线处理。

```
<AP>displaydiagnostic-information
[AP]_hidecmd
[AP-hidecmd]display ar5drv 2 radio
[AP-hidecmd]display ar5drv 2 statistics
[AP-hidecmd]display ar5drv 2 reset-log
[AP-hidecmd]display ar5drv 2 bss all
[AP-hidecmd]display ar5drv 2 channelbusy
[AP-hidecmd]display ar5drv 2 calibration
[AP-hidecmd]display ar5drv 2 queue all
[AP-hidecmd]display ar5drv 2 client all status
[AP-hidecmd]display ar5drv 2 client all rssi
[AP-hidecmd]display ar5drv 2 nf
[AP-hidecmd]display ar5drv 2 ani
```

上述信息隔 1 分钟再收集一次，共收集两次。

```
<AC>display wlan client mac-address XXXX-XXXX-XXXX verbose
<AC>wlan link-test XXXX-XXXX-XXXX        //多敲几次，直到有显示结果为止
```


无线CUPID定位故障排查
余 晨
表示上一步结果正常
表示上一步结果出现问题
开始
AP信号强度检查
能显示位置信息但精度不高
检查设备型号及定位基本配置
AP天线安装检查
无线网络优化并检查服务器日志
检查AP debug并在服务器上抓包确认AP发送定位包
AP部署检查
收集信息
检查定位服务器配置
拨打热线
400-810-0504
寻求帮助

1. 开始

基于 WLAN 的无线定位有多种技术实现途径，有基于信号传播模型的 RSSI 三角定位、RSSI 指纹定位，以及 H3C 私有的基于 RTT 光传输时延的三角定位(CUPID)。本云图专门针对 CUPID 定位的故障排查和处理。为保证定位精度，无线 CUPID 定位对 AP 部署、信号强度都有别于普通 Wi-Fi 部署的要求。在定位这类故障时，首先检查硬件部署，确认 AP 能正确发送定位报文，服务器定位进程是否正常启用并收发定位报文；其次就是检查无线网络环境及服务器配置，提高定位精度。

2. 流程图相关操作说明

(1) AP 信号强度检查

只有当大多数区域点位都能收到 4 个及以上 AP 的 Beacon 信号，并且强度大于－75dBm，方能保证较好的定位效果。所以定位要求 AP 有一定的部署密度。

(2) AP 天线安装检查

推荐使用普通全向天线，这类天线的辐射方向图比较稳定，且水平波瓣图接近于圆形，如图 7-16 所示。

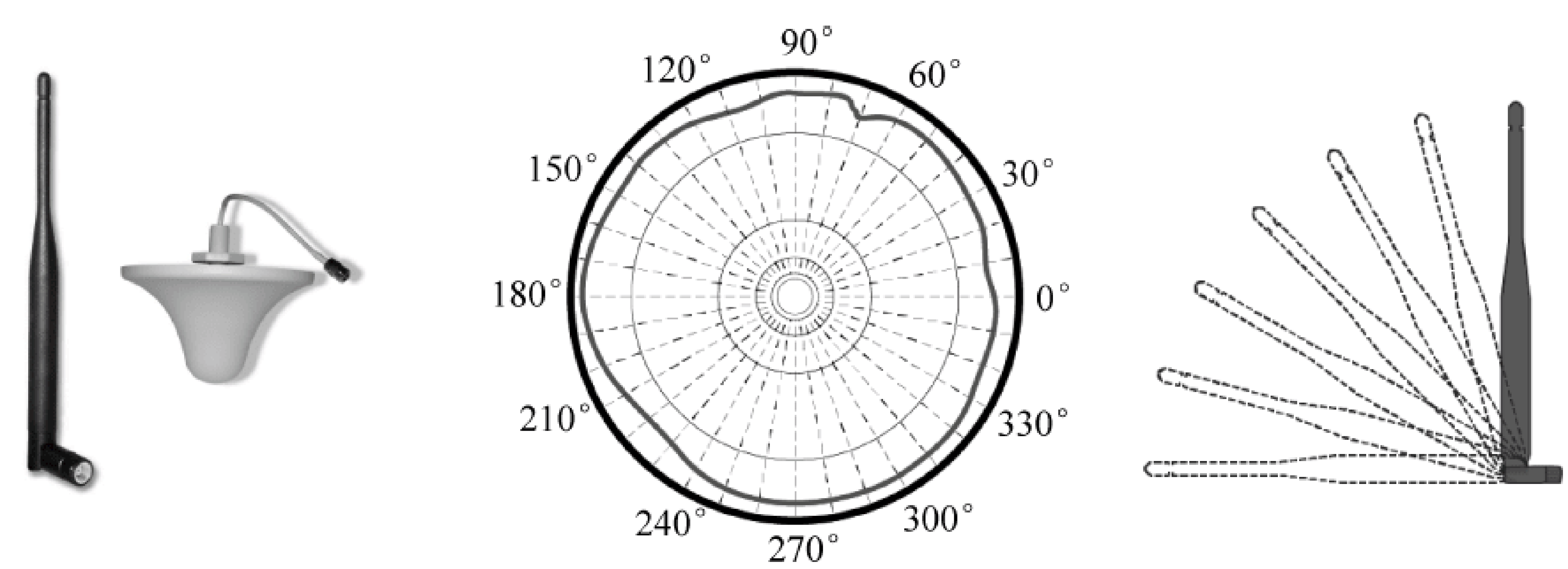


图 7-16 普通全向天线

对于有智能天线的 AP，比如 WA2620i-AGN、WA3620i-AGN 等，建议关闭智能天线功能。

命令：*undo smart-antenna enable*

例如：关闭 AP 智能天线。

```
 #
wlan ap b1-a01-i-2 model WA2620i-AGN id 102
  serial-id 210235A1BSC147001281
 undo broadcast-probe reply
 rfid-tracking engine-address 10.100.56.225
 radio 1 type dot11an
  channel 149
```

```
      service-template 2 vlan-id 80
    undo smart-antenna enable
  radio enable
  radio 2
    channel 1
    service-template 2 vlan-id 80
    undo smart-antenna enable
    radio enable
 #
```

（3）AP部署检查

当AP的部署不满足信号强度的要求时（即大多数区域都能收到4个及以上AP的Beacon信号并且强度大于－75dBm的要求），就需要考虑是否增加AP以及调整AP的部署位置。

① AP部署距离。为了保证AP的定位精度在5m以内，我们要求在进行AP部署的时候，需要做到相邻AP之间的间隔小于15m，保证至少4个AP可以覆盖到测试STA。

② 施工图纸要和定位用CAD图完全对应。施工图纸的实际AP位置要准确，如果有可能，拉网线时要留有一定的余量，方便后期进行点位微调。否则事后再处理操作会比较复杂。

③ 不同楼层之间注意类似天井那样的上下楼层通透的地方，AP部署的位置尽量远离这些区域。针对扶梯、天井等区域，在部署时为了避免定位错楼层，通常需要避开这些通透区域一定的距离。

④ 安装高度不宜过高，尽量控制在3m左右。AP安装的附近不要有明显的遮挡物，如金属等，尽量让AP的信号能够直射定位区域。

⑤ AP禁止安装在天花板内部，防止信号衰减太厉害。

（4）能显示位置信息但精度不高

确认故障的类别，是完全无法生成定位信息还是仅仅是定位精度不够高，比如误差普遍在15m以上。两类故障的定位思路完全不同：对于完全无法生成定位信息的情况，就需要排查AC的定位基础配置、AP型号是否支持定位，以及定位服务器配置是否正确。

（5）检查设备型号及定位基本配置

① 支持无线定位的设备情况（截至2015年6月）。CUPID当前只支持11n系列产品，其他未列进表格中的11n型号只要射频芯片型号符合条件也可以；部分较老的11n产品（如采用9160芯片）不支持。总的原则，只要是较新推出的11n产品（包括降成本包装的）都可以支持。11AC产品CUPID特性正在开发，将来会支持。支持CUPID定位的AC列举如表7-6所示。

表7-6　支持CUPID定位的AC举例

支持无线CUPID定位的AC	WX3000E、WX5004、WX6000系列及插卡、WX5500E、WX3500E 目前只在CMW V5上支持，B109D035及以上版本

支持 CUPID 定位的 AP 列举如表 7-7 所示。

表 7-7 支持 CUPID 定位的 AP 举例

类　　型	产品型号	CUP	2.4G	5G
第二代 11n 产品新 SOC WA2600V100R003	WA2620i-AGN	AR9350	SOC	AR59392
	WA2610i-GN	AR9350	SOC	
	WA1208E-ENP	AR9350	SOC	
	WA2610E-GNP	AR9350	SOC	
第二代 11n 产品降成本 SOC WA2600V100R005	WA2620E	AR9344	SOC	AR9582
	WA2610E	AR9344	SOC	
	WA2620X	AR9350	SOC	AR9592
	WA2610X	AR9350	SOC	
	WA2612	AR9344	SOC	
第一代 450M11n 产品室内型 WA3600V100R001	WA3628i-AGN	P1011	AR9390	AR9390
	WA3620i-AGN	P1011	AR9390	AR9390
	WA3610i-GN	P1011	AR9390	AR9390
面板式 AP WA2600V100R006	WA2610H-GN	AR9341	AR9341	NA

② 无线 CUPID 定位的基础配置。定位是否启用，AP 上报定位信息功能是否启用，配置 CUPID 定位模式，AP 模板下是否正确配置 iMC 定位服务器的地址，验证 AP 和 iMC 通信是否正常

```
<AC> system-view
[AC] wlan rfid-tracking enable
[AC] wlan rfid-tracking cupid ap-report enable
[AC] wlan rfid-tracking engine-type general mode cupid
[AC-wlan-ap-officeap1] rfid-tracking engine-address   xx.xx.xx.xx
```

(6) 检查 AP debug 并在服务器上抓包确认 AP 发送定位包

通过远程登录到 AP 上打开 CUPID 报文信息和 WLAN AS-Location 信息。如果能抓到相关 debug，说明 AP 能正常发送定位包。

命令：*[AP01-hidecmd]debugging ar5drv 1/2 cupid info*

[AP01-hidecmd]debugging ar5drv 1/2 cupid error

<AP01>debugging wlan as-location all

telminal debugging

telminal monitor

```
* Mar  4 17:21:00:991 2015 f2-a01-i-1 WASL/7/EVENT :
Client 4cac-0a45-5043 rssi is 47 and nf is 106.
* Mar  4 17:21:00:991 2015 f2-a01-i-1 WASL/7/FRAME : Put MU message into the queue.
* Mar  4 17:21:00:995 2015 f2-a01-i-1 WASL/7/EVENT :WASL begin to send frame to server.
* Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/EVENT :
WASL report ip address is 10.100.56.225.
* Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/EVENT :
WASL report port is 1144.
```

```
 * Mar  4 17:21:00:996 2015 f2-a01-i-1 WASL/7/VERBOSE : AE message:
  00 01 01 26 18 e8 5a 48 00 01 00 01 4c ac 0a 45
  50 43 74 25 8a 86 f0 a0 02 00 74 25 8a 86 f0 b0
  00 00 0b 00 ba b6 b1 f1 c5 96 00 50 00 21 00 00
 2d 1a 8c 01 1b ff 00 00 00 00 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 33 1a 8c 01
  1b ff 0
 * Mar  4 17:21:00:997 2015 f2-a01-i-1 WASL/7/EVENT : WASL send frame to server.
 * Mar  4 17:21:00:997 2015 f2-a01-i-1 WASL/7/EVENT :Send message to AE successfully.
 * Jun  7 21:58:51:061 2015 ap3 WDP/7/debug2:
 Tx:Sta_mac_addr= 18F6431B38F5, channel=161, tod=7649,retries=0,Tx_status=4
 * Jun  7 21:58:51:061 2015 ap3 WDP/7/debug2:
 SendMsg to Server:Sta_mac_addr=18F6431B38F5, channel=161, tod=13281,toa=14951,toa-tod=
 1670,numOfChains=3,rssi1=27,rssi2=38,rssi3=43
 * Jun  7 21:58:51:062 2015 ap3 WDP/7/debug2:
 Tx:Sta_mac_addr= 18F6431B38F5, channel=161, tod=63147,retries=0,Tx_status=4
 * Jun  7 21:58:51:062 2015 ap3 WDP/7/debug2:
 Tx:Sta_mac_addr= 18F6431B38F5, channel=161, tod=103472,retries=0,Tx_status=4
 * Jun  7 21:58:51:062 2015 ap3 WDP/7/debug2:
 Tx:Sta_mac_addr= 18F6431B38F5, channel=161, tod=127772,retries=0,Tx_status=4
```

通过在 AP 上行口或者直接在服务器上抓包也能判断，AP 发送定位报文的目标 IP 地址为定位引擎服务器 IP 地址，端口号 1144。基于 Wireshark 的 CUPID 协议解析的插件（“DMP”→“技术支持中心”→“01IP 网络产品”→“20 无线产品”→“13 无线定位”→“02CUPID 定位”），能够快速分析，如图 7-17 所示。

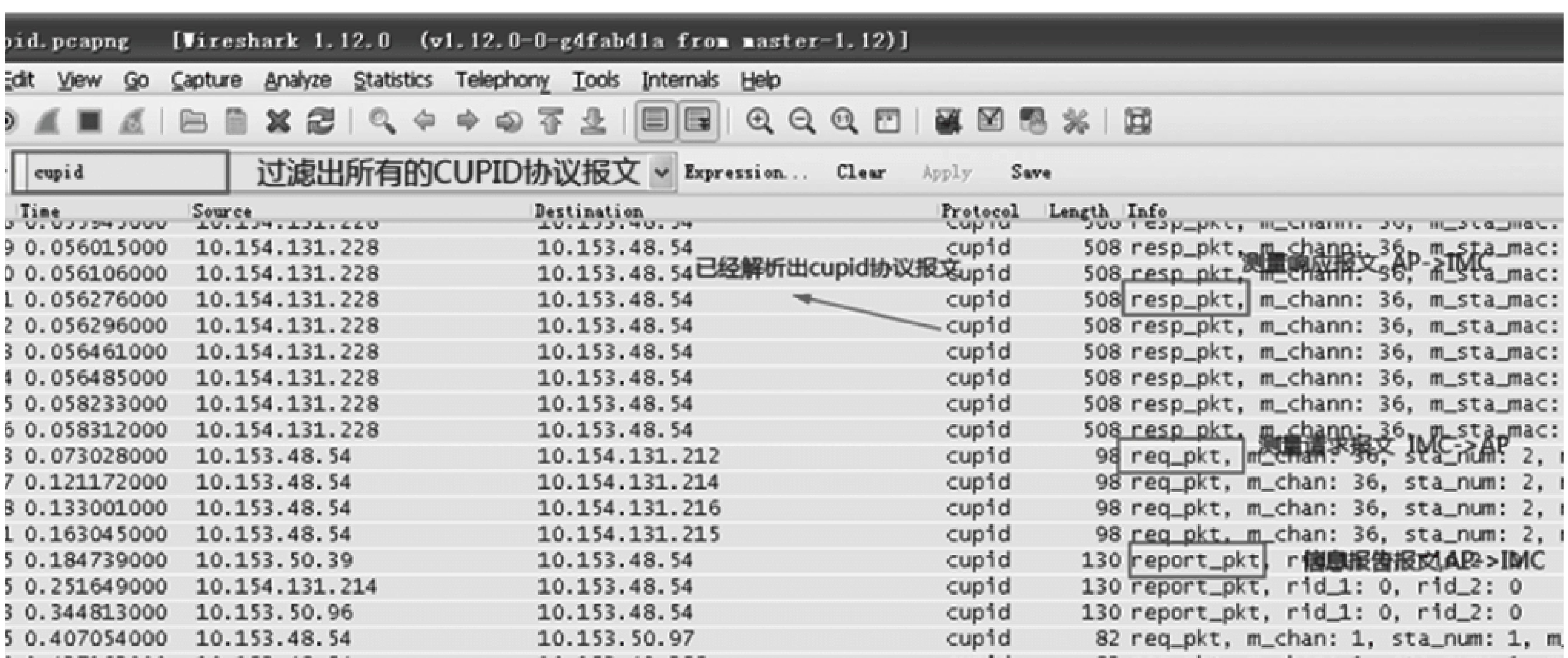


图 7-17　基于 Wireshark 的 CUPID 协议解析

三类 CUPID 报文如下。

CUPID. report AP 主动上报关联终端的报文。

CUPID. req 服务器给 AP 发送的测量请求报文。

CUPID. resp AP 给服务器回应的测量报文。

（7）检查定位服务器配置

检查定位服务器上的 IMC 定位进程是否启用，检查定位服务器近期有没有调整过配置，包括是否有 IP 地址变更、定位参数调整等。检查定位服务器到 AP 的网络路由是否可达。

① 定位进程 imclocatedm 和调度进程 imclocatemgrdm 正常启用，如图 7-18 所示。

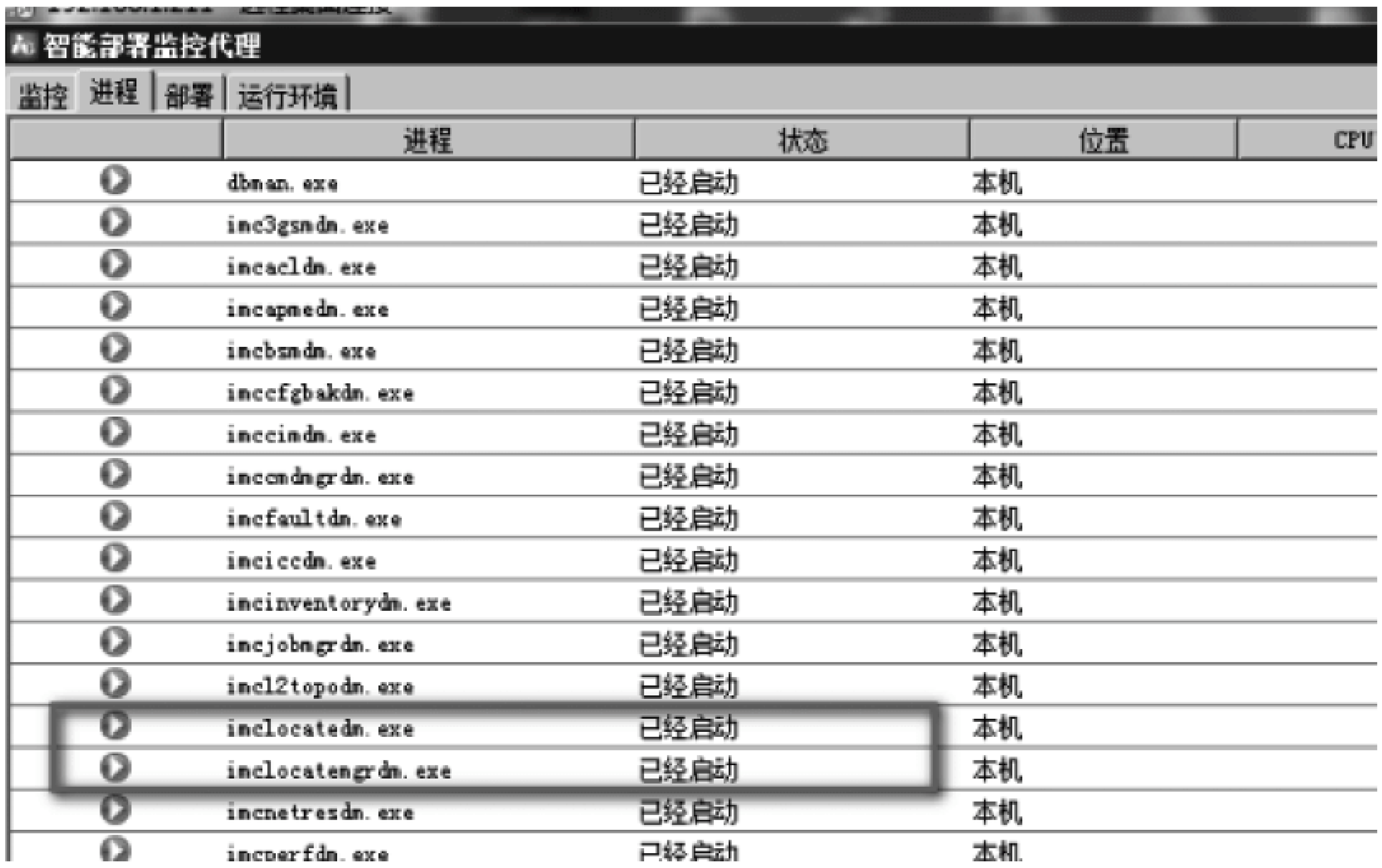


图 7-18　定位进程 imclocatedm 和调度进程 imclocatemgrdm 正常启用

② 检查定位配置文件。配置文件（“iMC”→“server”→“conf”→“imc_locate.conf”）中参数主要用于定位系统调优和问题分析，正常情况下不需要修改。MaxLocateApSquareDis 为最远的两个 AP 距离的平方，默认为 MaxLocateApSquareDis＝900，即参与定位的 4 个 AP 中相邻最远的两个 AP 距离为 30m，如图 7-19 所示。若为 40m，则设置 MaxLocateApSquareDis＝1600。

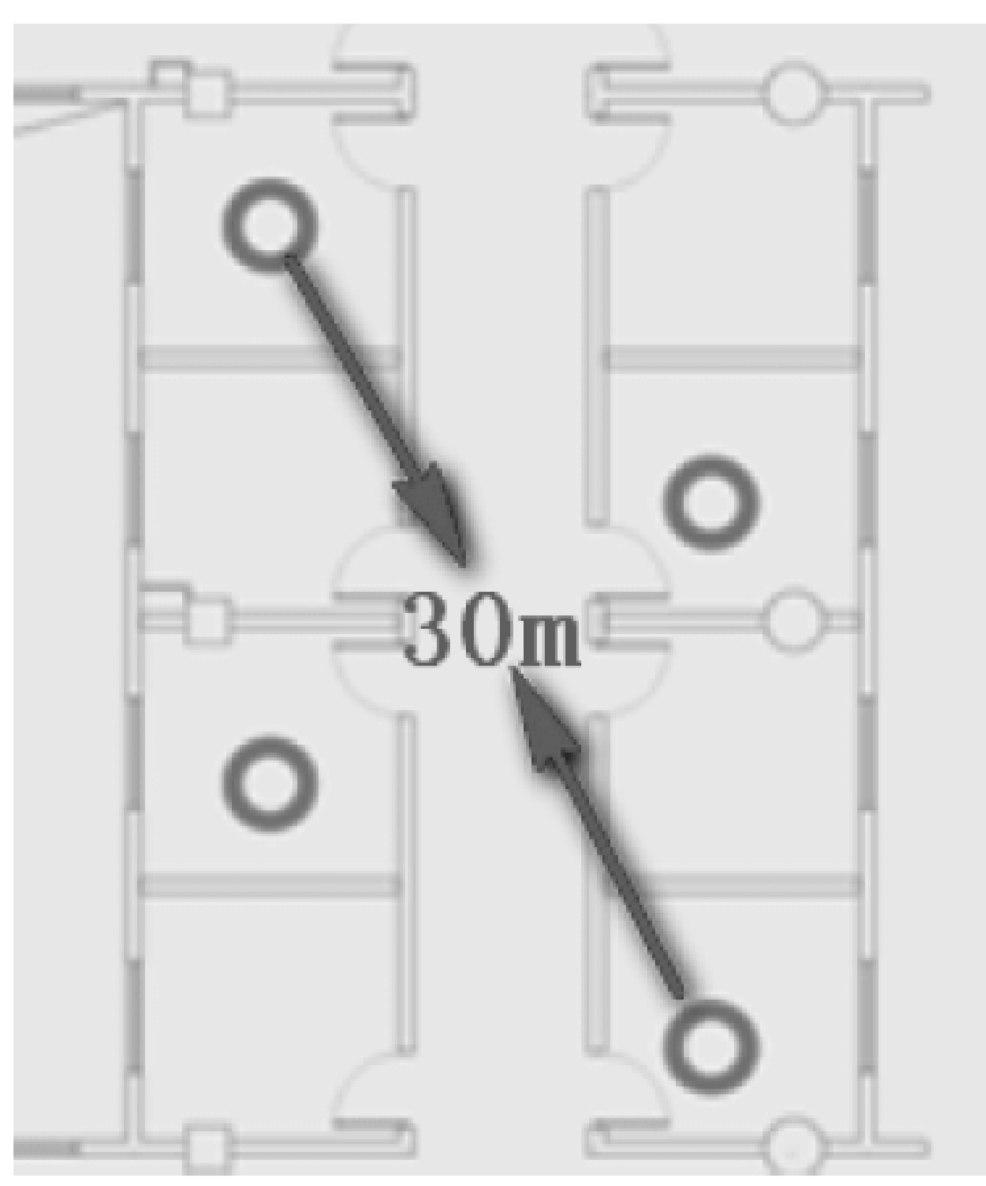


图 7-19　相邻最远的两个 AP 距离为 30m

（8）无线网络优化并检查服务器日志

① 定位过程是通过 AP 发送低速报文来进行计算的，而低速报文在发送过程当中对空口资源的消耗是比较大的，发送过程中也会因为竞争和干扰等问题降低了定位报文的发送成功率，参考无线通用优化指导对空口进行监控并优化。

② 检查服务器定位日志。

通过“iMC”→“server”→“conf”→“log”→“imclocatedm.txt”日志分析原因，查找

“locateAP”关键字，检查参与定位的 AP 数是否至少为 4 个。

（表示如果某个 sta 关联在 oAssAp：apname1 上，那么参与定位的 AP 为 locateAP：apname1 apname2 apname3 apname4。）

```
2015-05-30 13:10:24.118 [INFO (0)] [THREAD(9224)] [CLocateProcessor::addMasterSubMap]
(Info) oAssAp: test2 locateAP: test3 test2 test5 test4
2015-05-30 13:10:24.118 [INFO (0)] [THREAD(9224)] [CLocateProcessor::addMasterSubMap]
(Info) oAssAp: test3 locateAP: test3 test2 test5 //参与定位的 AP 数少于 4 个，检查 test4 的覆盖情况
2015-05-30 13:10:24.118 [INFO (0)] [THREAD(9224)] [CLocateProcessor::addMasterSubMap]
(Info) oAssAp: test4 locateAP: test3 test2 test5 test4
2015-05-30 13:10:24.118 [INFO (0)] [THREAD(9224)] [CLocateProcessor::addMasterSubMap]
(Info) oAssAp: test5 locateAP: test3 test2 test5 test4
```

（9）收集信息

① 服务器侧打开 debug 开关，“iMC”→“server”→“conf”→“imc_locate.conf”设置如下。

DebugSta＝all

PrintSendMsg＝true

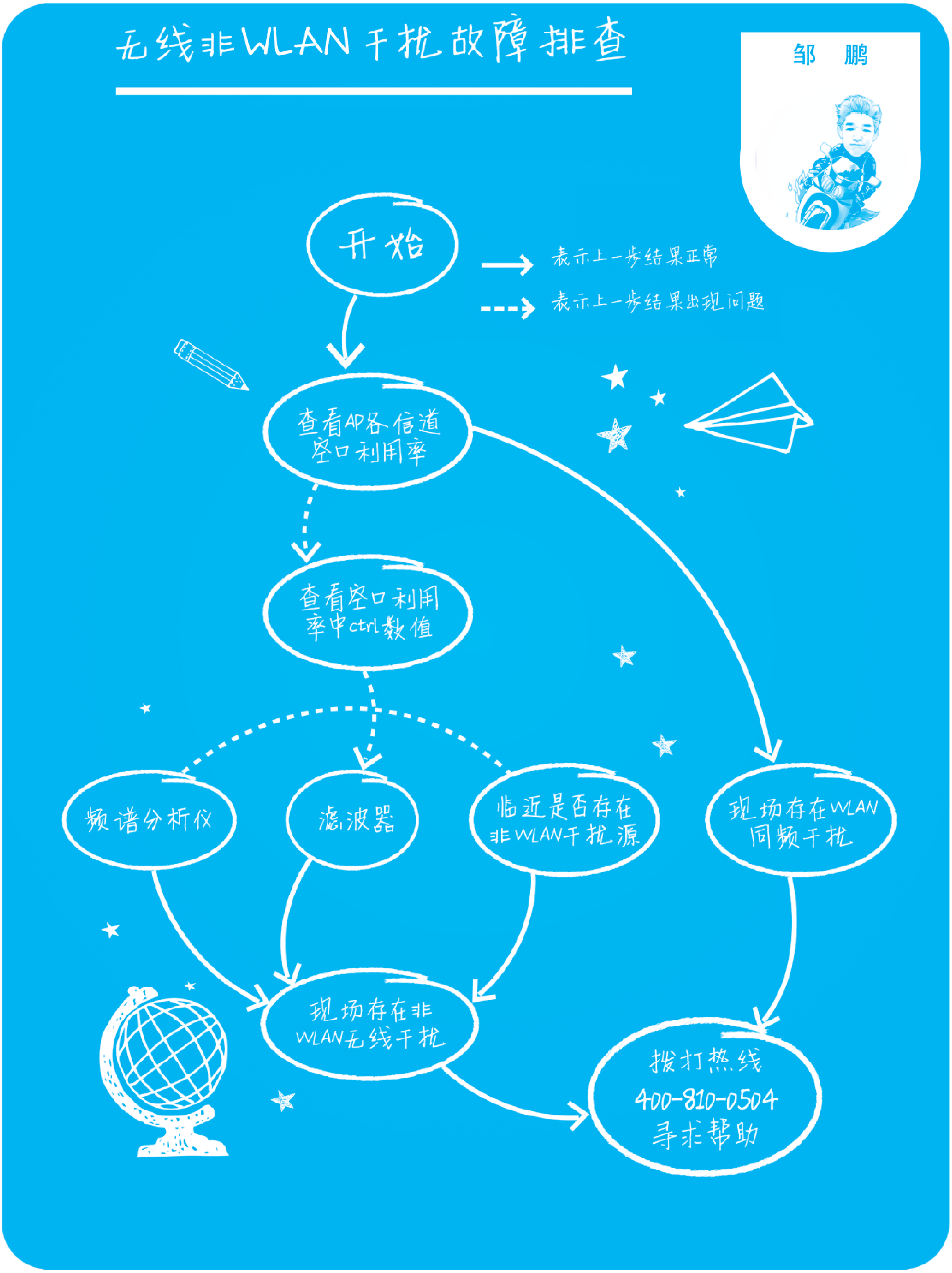
② AC 配置信息、AP 空口信息。

③ iMC 定位效果截图（显示 MAC 地址）。

④ 收集服务器 iMC\server\conf\log\ 目录下文件 imclocatemgrdm 和 imclocatedm 和 imc\server\conf\POS\ 目录下所有的文件。

⑤ 收集 WSM 服务器上的 5MB 以内的抓包。

将以上信息反馈 800 处理。


无线非WLAN干扰故障排查
邹 鹏
开始
表示上一步结果正常
表示上一步结果出现问题
查看AP各信道空口利用率
查看空口利用率中ctrl数值
频谱分析仪
滤波器
临近是否存在非WLAN干扰源
现场存在WLAN同频干扰
现场存在非WLAN无线干扰
拨打热线
400-810-0504
寻求帮助

1. 开始

无线非 WLAN 干扰定位故障的思路是：先检查 AP 空口利用率是否具有显著的非 WLAN 干扰特点，再通过滤波器、频谱分析仪、检查现场环境等方法验证。

2. 流程图相关操作说明

(1) 查看 AP 射频口上各信道的空口利用率是否过高

登录到 AP 上进入隐藏模式查看 2.4G 射频各信道(1、6、11)的空口利用率信息是否过高，CtlBusy 的值是否高于 60%。

命令：

① 登录到 AP 上进入隐藏模式。

[*H3C*] *_hide*

② 查看 AP 当前信道的空口利用率。

[H3C-hidecmd] *display ar5 2 channelbusy*

例如：通过命令查看指定 AP 当前信道的空口利用率。

```
[11f04-hidecmd]display ar5 2 channelbusy
ChannelBusy information
 Ctl Channel:      06      Channel Band: 20M
 Ext Channel:
 Record Interval(s):    9
 Date/Month/Year: 13/05/2015
          Time(h/m/s):     CtlBusy(%)   TxBusy(%)   RxBusy(%)   ExtBusy(%)
 01        07:20:59          80           6           26           0
 02        07:20:50          87           6           25           0
 03        07:20:41          84           6           22           0
 04        07:20:32          83           6           23           0
 05        07:20:23          89           6           29           0
 06        07:20:14          80           6           29           0
 07        07:20:05          83           7           21           0
 08        07:19:56          86           9           20           0
 09        07:19:47          85           6           23           0
 10        07:19:38          80           6           24           0
 11        07:19:29          82           4           22           0
 12        07:19:20          80           5           22           0
 13        07:19:11          82           0           24           0
 14        07:19:02          85           4           20           0
 15        07:18:53          83           4           22           0
 16        07:18:44          85           4           22           0
 17        07:18:35          86           4           26           0
 18        07:18:26          80           4           20           0
 19        07:18:17          57           4           47           0
 20        07:18:08          54           4           46           0
```

(2) 查看空口利用率中数据是否具有典型非 WLAN 干扰特征

查看 AP 当前信道空口利用率中 CtlBusy 的数值是否远大于 Tx 与 Rx 之和。一般差值大于 30%即为非 WLAN 干扰的典型特征。

例如：通过命令查看，当前 AP 的空口利用率 CtlBusy 已经大于 60%，属于信道繁忙，且 Ctlbusy 的数值远大于 Tx 与 Rx 之和。

```
[11f04-hidecmd]display ar5 2 channelbusy
ChannelBusy information
 Ctl Channel:      06      Channel Band: 20M
 Ext Channel:
 Record Interval(s):   9
 Date/Month/Year: 13/05/2015
       Time(h/m/s):    Ctlbusy(%)   TxBusy(%)   RxBusy(%)   ExtBusy(%)
 01     07:20:59          80            6           26           0
 02     07:20:50          87            6           25           0
 03     07:20:41          84            6           22           0
 04     07:20:32          83            6           23           0
 05     07:20:23          89            6           29           0
 06     07:20:14          80            6           29           0
 07     07:20:05          83            7           21           0
 08     07:19:56          86            9           20           0
 09     07:19:47          85            6           23           0
 10     07:19:38          80            6           24           0
 11     07:19:29          82            4           22           0
 12     07:19:20          80            5           22           0
 13     07:19:11          82            0           24           0
 14     07:19:02          85            4           20           0
 15     07:18:53          83            4           22           0
 16     07:18:44          85            4           22           0
 17     07:18:35          86            4           26           0
 18     07:18:26          80            4           20           0
 19     07:18:17          57            4           47           0
 20     07:18:08          54            4           46           0
```

（3）现场测试验证存在非 WLAN 的无线干扰

由于无线环境较为脆弱，尤其是 2.4G 频段干扰源较多，运营商 4G、微波炉等都会造成对 WLAN 的干扰，若怀疑是非 WLAN 的干扰可以采用下列方式进行确认。

① 使用频谱分析仪扫描现场无线环境。通过使用专业的无线勘测仪器——频谱分析仪配合高性能天线对现场无线环境进行勘测，尤其是 2.4G 临近频段的信号波动。如果有较为强烈的电磁波信号，可以判断临近有较为强烈的干扰源，如图 7-20 所示。

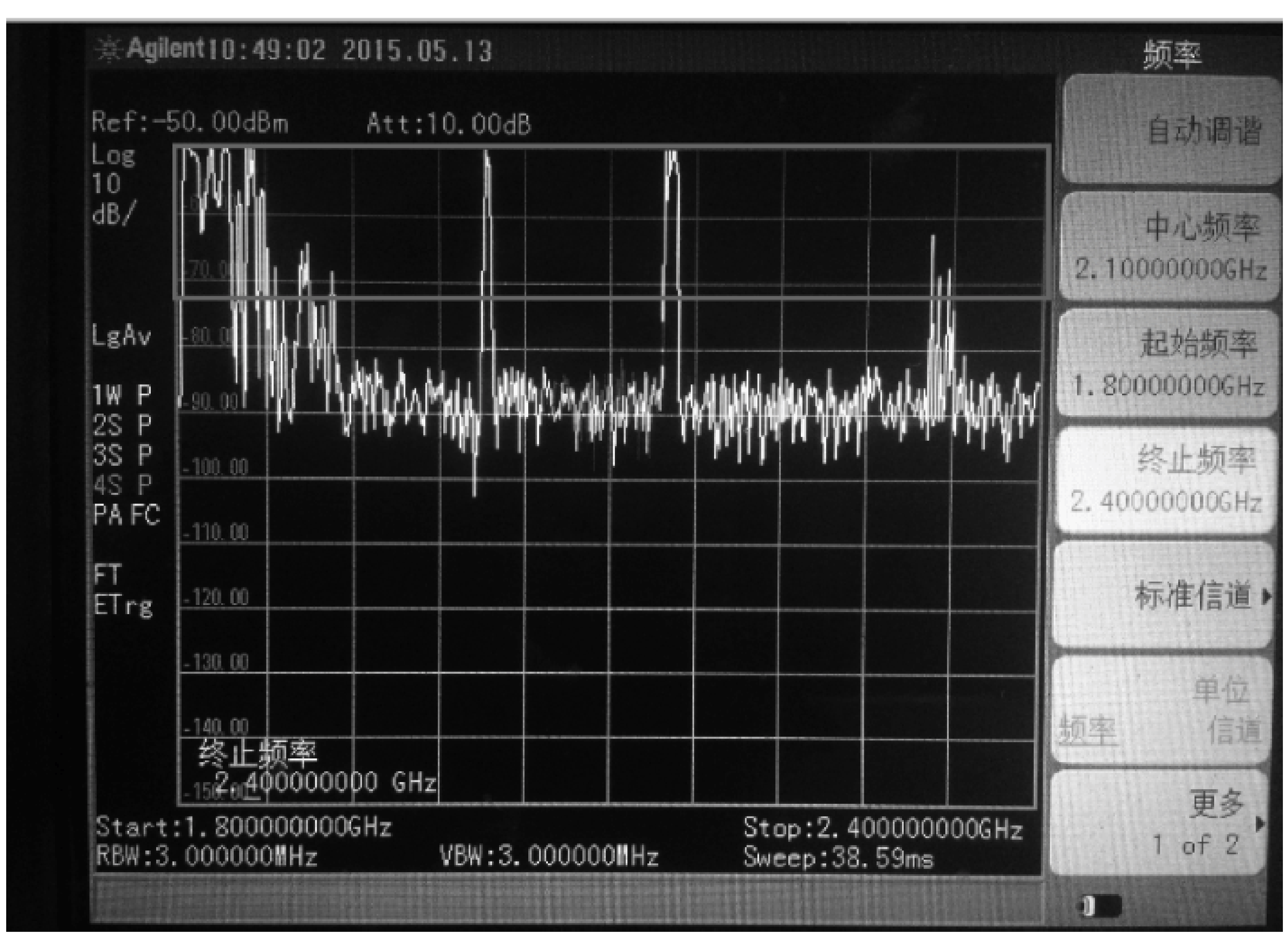


图 7-20　频谱分析仪

② 通过在现有 AP 上加装滤波器，对比加装前后的空口利用率来确认非 WLAN 干扰源。滤波器属于有源设备，需要加装在 AP 与天线之间，通过过滤固定频段的电磁波来达到屏蔽干扰的效果，市面上滤波器的规格参差不齐，一般选取过滤 2.4GHz 临近频段的滤波器为宜，如图 7-21 所示。

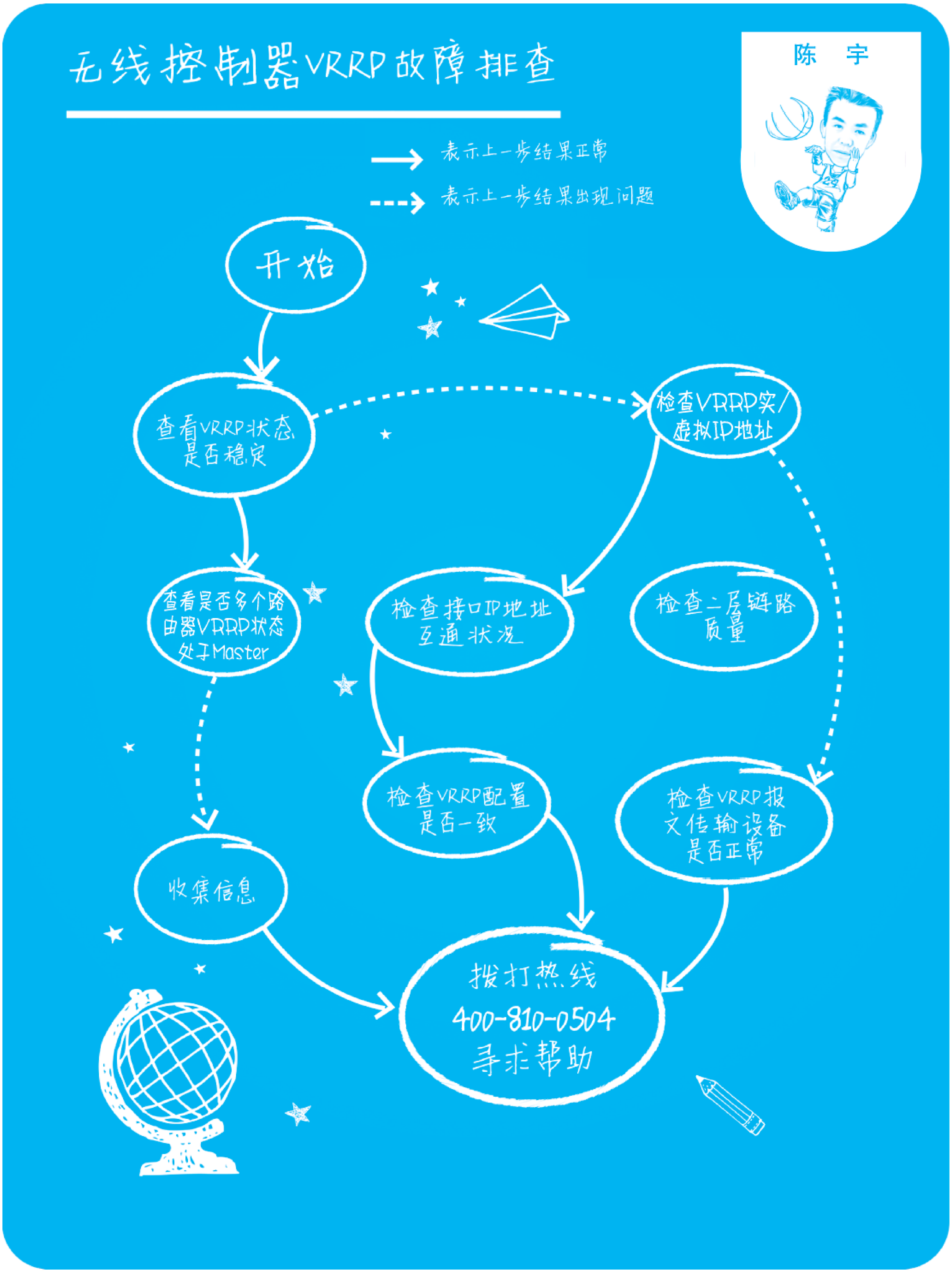


图 7-21 滤波器

③ 通过现场观察与交流确认是否存在非 WLAN 的干扰源。通过对现场的观察，如果 AP 部署的临近有明显的非 WLAN 干扰源，比如运营商天线或微波炉等，尤其是无线使用问题出现前后环境有变动，比如运营商开了 4G，则可以判断现场存在非 WLAN 的无线干扰，如图 7-22 所示。



图 7-22 非 WLAN 的干扰源


无线控制器VRRP故障排查
陈 宇
表示上一步结果正常
表示上一步结果出现问题
开始
查看VRRP状态是否稳定
检查VRRP实/虚拟IP地址
查看是否多个路由器VRRP状态处于Master
检查接口IP地址互通状况
检查二层链路质量
检查VRRP配置是否一致
检查VRRP报文传输设备是否正常
收集信息
拨打热线
400-810-0504
寻求帮助

1. 开始

首先观察备份组 VRRP 状态是否稳定。如果状态稳定，则先检查 VRRP 接口实 IP 地址能否互通，再检查 VRRP 配置是否正确，最后查看协议报文的发送状况；如果状态频繁切换，则先检查收发 VRRP 报文所在 VLAN 的二层链路是否稳定，再检查 CPU 占用率是否正常，最后检查 VRRP 报文发送时间间隔是否过短。

2. 流程图相关操作说明

(1) 查看 VRRP 状态是否稳定

路由器在备份组中的状态可以为 Master、Backup 和 Initialize。检查 VRRP 状态是否存在 Master/Backup 频繁切换的情况。

命令：*display vrrp*

例如：通过命令查看，可以确认路由器的 VRRP 状态为 Backup。

```
<Backup_DEV>display vrrp
 IPv4 Standby Information:
     Run Mode: Standard
     Run Method: Virtual MAC
 Total number of virtual routers : 1
 Interface          VRID   State        Run     Adver    Auth       Virtual
                                        Pri     Timer    Type         IP
 -------------------------------------------------------------------------------
 Vlan1              1      Backup       100     1        Simple     1.1.1.254
```

(2) 查看是否多个路由器 VRRP 状态处于 Master

分别查看每台路由器备份组的 VRRP 状态信息，是否备份组中存在多个路由器 VRRP 状态处于 Master。

(3) 检查接口是否 Up

检查运行 VRRP 的 VLAN 虚接口是否 Up。

命令：*display interface interface-type interface-number*

例如：通过命令查看 VLAN 1 三层虚接口状态是否 Up。

```
<Master_DEV>display interface Vlan-interface 1
Vlan-interface1 current state:Down
Line protocol current state:Down
Description: Vlan-interface1 Interface
...
```

(4) 检查 VRRP 实/虚拟 IP 地址

确保运行 VRRP 的端口 Up 的前提下，查看 VRRP 的虚拟 IP 是否与端口实 IP 在同一网段。

例如：如果实 IP 与虚拟 IP 不在同一网段，则 VRRP 状态为 Initialize。

```
[Master_DEV-Vlan-interface1]display this
#
interface Vlan-interface1
 ip address1.1.1.252 255.255.255.0
 vrrp vrid 1 virtual-ip1.1.100.254
 vrrp vrid 1 virtual-ip 1.1.100.254
```

(5) 检查接口 IP 地址互通状况

如果互 ping 接口 IP 地址不通，主要检查以下内容。

① 检查接口是否 Up，链路是否故障。

② 如果物理接口是 Access 端口，是否与 VRRP 备份组属于同一 VLAN；如果是 Trunk 或者 Hybrid 端口，端口的 PVID 是否一致，是否允许 VRRP 备份组所在 VLAN 通过。

③ 端口下是否开启了认证、ACL 过滤等安全功能。

(6) 检查 VRRP 配置是否一致

主要检查内容包括：运行模式、VRID、VRRP 报文发送间隔时间、抢占模式、认证方式和认证字的配置是否相同。

命令：*display vrrp verbose*

例如：通过命令查看，观察 Master 和 Slave 的相关参数是否一致。

```
<Master_DEV>display vrrp verbose interface Vlan-interface 1
 IPv4 Standby Information:
     Run Mode          : Standard
     Run Method        : Virtual MAC
 Total number of virtual routers on interface Vlan1 : 1
   Interface Vlan-interface1
     VRID              : 1                Adver Timer : 2
     Admin Status      : Up               State       : Master
     Config Pri        : 120              Running Pri : 120
     Preempt Mode      : Yes              Delay Time  : 0
     Auth Type         : Simple           Key         : ******
     Virtual IP        : 1.1.1.254
     Virtual MAC       : 0000-5e00-0101
     Master IP         : 1.1.1.253
```

(7) 检查二层链路质量

① 检查互连端口是否有错误报文的增长。

② 检查链路状况是否有震荡，是否有端口频繁 Up/Down。

③ 使用 VRRP 接口的实 IP 地址互 ping 时是否有回应超时。

④ 如果是光介质，检查光衰减是否在正常范围之内。

(8) 检查 VRRP 报文传输设备是否正常

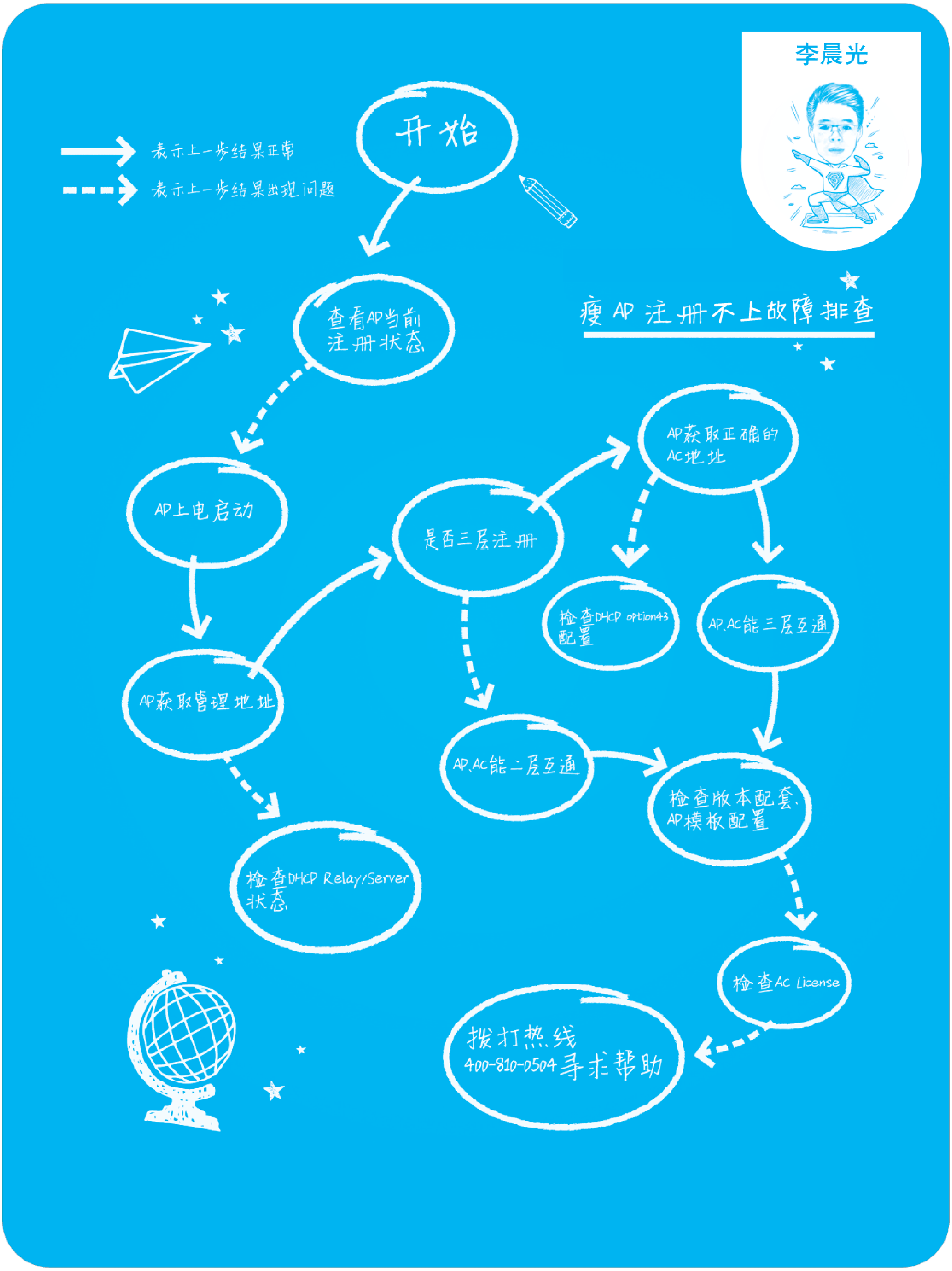
在中间设备或互连接口做流量统计，检查是否有 VRRP 报文从接口发出或接收。如果要检查是否正常发出了 VRRP 报文，则在接口的 Outbound 方向进行流量统计；如果要检查是否正常接收了 VRRP 报文，则在接口的 Inbound 方向进行流量统计。

命令：*display qos policy interface interface-type interface-number*

例如：通过匹配目的地址为 224.0.0.18、协议号为 112 的 VRRP 报文，对这一类型的报文在接口下做 Inbound 方向流量统计，观察 VRRP 报文的接收情况是否正常。

```
[H3C]display current-configuration
...
acl number 3000
 rule0 permit 112 source 1.1.1.252 0 destination 224.0.0.18
#
traffic classifierACT operator and
 if-match acl 3000
#
traffic behaviorACT
 accounting
#
qos policyACT
 classifierACT behavior ACT
#
interface GigabitEthernet3/0/1
qos apply policyACT inbound

[H3C]display qos policy interface GigabitEthernet 3/0/1
  Interface: GigabitEthernet3/0/1
  Direction:Inbound
  Policy:ACT
   Classifier:ACT
     Operator: AND
     Rule(s) : If-match acl 3000
     Behavior:ACT
      Accounting Enable:
        51 (Packets)
```


李晨光
瘦 AP 注册不上故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看AP当前注册状态
AP上电启动
AP获取管理地址
检查DHCP Relay/Server状态
是否三层注册
AP获取正确的AC地址
检查DHCP option43配置
AP.AC能三层互通
AP.AC能二层互通
检查版本配套.AP模板配置
检查AC License
拨打热线 400-810-0504寻求帮助

1. 开始

FIT AP、AC 是通过三层 IP 网络构建 CAPWAP 隧道来完成注册的。所以定位故障的思路是：先确保 AP、AC 在 IP 层能正常通信，再检查版本、配置、License 等信息。

2. 流程图相关操作说明

(1) 查看 AP 当前注册状态

命令：*display wlan ap all*

例如：State 为"I"表示 AP 未上线；"R/M""R/B"表示 AP 已上线，分别为主、备隧道。

```
<H3C>display wlan ap all
...
State :I = Idle,    J = Join, JA = JoinAck,    IL = ImageLoad
          C = Config, R = Run,   KU = KeyUpdate, KC = KeyCfm
-----------------------------------------------------------------------
 AP Name                          State  Model            Serial-ID
-----------------------------------------------------------------------
 fz_dgl_001                       I      WA1208E-GP       210235A0A9C094001953
 fz_dgl_002                       R/M    WA1208E-GP       210235A0A9C094001529
 fz_dgl_003                       R/B    WA2100           210235A22WB093001434
```

(2) AP 上电启动

如果 AP 无法注册上线，首先需要检查 AP 是否成功上电启动。分两种场景。

① 现场定位。在现场定位时，可以直接通过观察 AP 电源指示灯，或者观察接入交换机端口指示灯状态来确定 AP 是否正常启动。

② 远程定位。在远程定位时，可以通过观察和 AP 同二层网的设备能否学习到 AP MAC 地址来辅助判断，如果接入交换机未能学习到 AP MAC 地址，可能是 AP 未启动，或者连接 AP 网线存在故障。

命令：*display mac-address*

例如：在接入交换机上查看 MAC 表，如果有学习到 AP MAC 地址，可以确定 AP 已启动。

```
<H3C>display mac-address
MAC ADDR         VLAN ID    STATE       PORT INDEX              AGING TIME(s)
0023-8999-fec0   4000       learned     Bridge-Aggregation1     AGING
0023-8999-fde0   4000       learned     Bridge-Aggregation1     AGING
```

另外，如果 AP 是 POE 供电方式，则根据 POE 交换机的供电情况也能确定 AP 是否上电启动。

命令：*display poe interface*

例如：查看 POE 交换机端口供电，正常情况 AP 功耗会超过 5W，否则 AP 可能未正常启动。

```
<SW>display poe interface
 Interface    Status    Priority CurPower Operating  IEEE   Detection
                                 (W)      Status     Class  Status
 GE1/0/1      enabled   low      7.2      on         3      delivering-power
 GE1/0/2      enabled   low      3.2      on         3      delivering-power
```

如果最终定位到 AP 未启动，则需要检查本地供电电源或者 POE 交换机、网线等。必要时可以尝试替换网线、POE 交换机或者 AP 来确认故障点。

(3) AP 获取管理地址

AP 启动后需要获取管理 IP 地址，可以通过查看 DHCP Server 状态，确定服务器有没有给 AP 分出去地址。

命令：*display dhcp server ip-in-use pool ap_01*

```
<H3C>display dhcp server ip-in-use pool ap_01
Pool utilization: 46.74%
 IP address       Client-identifier/     Lease expiration           Type
                  Hardware address
 192.168.86.166   0023-8999-fec0      Apr 22 2013 02:13:18       Auto:COMMITTED
 192.168.86.97    3822-d694-2200      Apr 22 2013 02:20:46       Auto:COMMITTED
```

(4) 检查 DHCP Relay/Server 状态

查看 AP 的管理 DHCP 地址池配置是否正确，地址池是否够用，是否有地址冲突等。

命令：*display dhcp server tree pool xxx*

```
<H3C>display dhcp server tree pool
Global pool:

Pool name: cdwlan
 network192.168.86.0 mask 255.255.252.0
 PrevSibling node:0
 gateway-list192.168.86.2
 expired 1 0 0 0
```

命令：*display dhcp server ip-in-use pool xxx*

例如：通过命令查看 DHCP 利用率，超过 90%就需要关注了。

```
<H3C>display dhcp server ip-in-use pool ap_01
Pool utilization: 46.74%
 IP address       Client-identifier/     Lease expiration           Type
                  Hardware address
 192.168.86.166   0023-8999-fec0      Apr 22 2013 02:13:18       Auto:COMMITTED
 192.168.86.97    3822-d694-2200      Apr 22 2013 02:20:46       Auto:COMMITTED
```

命令：*display dhcp server conflict all*

```
<H3C>display dhcp server conflict all
    Address            Discover time
    192.168.86.3       Apr  9 2013 12:19:32
    192.168.86.4       Apr  9 2013 12:19:32
```

(5) 是否三层注册

根据用户的实际组网情况检查确定 AP、AC 注册方式。

在二层、三层不同注册方式下，AP 发现并注册 AC 的方式不一样，问题排查的方向也不同。

(6) AP、AC 能二层互通

此步骤可以通过 AC ping AP。需要注意的是，CAPWAP 隧道对 AP-AC 之间的链路丢包比较敏感，要求有线丢包率小于 0.1%。同时链路要支持 MTU 1500。

命令：*ping -s 1472 -f x.x.x.x*

例如：ping 1472 字节包(MTU 1500)，强制不分片，检测 AP-AC 链路。

```
<AC>ping -s 1472 -f 192.168.86.166
  PING192.168.86.166: 1472  data bytes, press CTRL_C to break
    Reply from192.168.86.166: bytes=1472 Sequence=1 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=2 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=3 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=4 ttl=21 time=20 ms
```

如果二层互通性有问题，检查 AP、AC 二层组网，排查物理链路、VLAN 配置、STP 状态等。

(7) AP 获取正确的 AC 地址

三层注册中，AP 常用两种方式获取 AC 地址。

① 通过 DHCP Option 43 选项。

命令：*display dhcp client verbose*

例如：通过命令查看，可以确认 AP 获取的 Boot Server 地址是否为 AC 地址。

```
<AP>display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP:192.168.86.166 255.255.252.0
 Allocated lease: 864000 seconds, T1: 432000 seconds, T2: 756000 seconds
 Lease from 2013.04.20 23:23:47    to    2013.04.30 23:23:47
 DHCP server:192.168.86.50
 Transaction ID: 0x6249fa29
 Default router: 192.168.86.1
 Boot server: 10.21.100.10
 Client ID:0023-8999-fec0
 T1 will timeout in 4 days 11 hours 34 minutes 57 seconds.
```

② 手动在 AP 上设置 WLAN AC IP。

命令：*wlan ac ip x.x.x.x*

例如：检查 AP 是否配置正确的 WLAN AC IP 地址

```
<AP>display current-configuration
#
wlan ac ip 10.21.100.10
#
```

(8) 检查 DHCP Option 43 配置

对于通过 DHCP Option 43 方式获取 AC 注册地址的情况，需要确保 DHCP Server 的 Option 43 参数配置正确。

命令：*display dhcp server tree all*

```
<H3C>display dhcp server tree all
Global pool:

Pool name: 1
  network 192.168.86.0 mask 255.255.252.0
  Sibling node:2
  gateway-list192.168.86.1
  option 43 hex 800B0000 020A1564 0A0A1564 07
  expired 10 0 0
```

说明：当修改 DHCP Server 配置后需要让 AP 重新获取地址，新配置才能生效。

Option 43 格式简要说明如图 7-23 所示。

```
80 0B 00 00 02 0A 15 640A 0A 15 64 07
80：固定值，不用改变；
0B：长度字段，其后面所跟数据的字节长度；
00 00：固定值，不用改变；
02：表示后面的 IP 地址的个数，此处为二个 IP 地址；
0A 15 64 0A：十六进制转十进制为 IP 地址一 10.21.100.10
0A 15 64 07：十六进制转十进制为 IP 地址二 10.21.100.7
```

图 7-23　Option 43 格式简要说明

(9) AP、AC 能三层互通

此步骤可以通过 AC 带源(Option 43 指定的接口地址)ping AP 来测试。需要注意的是，CAPWAP 隧道对 AP-AC 之间的链路丢包比较敏感，要求有线丢包率小于 0.1%。同时链路要支持 MTU 1500。

命令：*ping -a x.x.x.x*(AC 注册地址) *-s 1472 -f x.x.x.x*(AP 地址)

例如：ping 1472 字节包(MTU 1500)，强制不分片，检测 AP-AC 链路。

```
<AC>ping -a 10.21.100.10 -s 1472 -f 192.168.86.166
  PING192.168.86.166: 1472   data bytes, press CTRL_C to break
    Reply from192.168.86.166: bytes=1472 Sequence=1 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=2 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=3 ttl=21 time=20 ms
    Reply from192.168.86.166: bytes=1472 Sequence=4 ttl=21 time=20 ms
```

如果三层互通性有问题，需要排查 AP 到 AC 的三层路由，保证 IP 层互通。

(10) 检查版本配套、AP 模板配置

如果 AP、AC 在 IP 层通信正常，但仍无法正常注册时排查方法如下。

① 查看 AC、AP 版本是否匹配。

第一，检查 AC Flash 是否有瘦 AP 的版本文件，如果没有，上传正确的 AP 版本文件至 AC Flash；

第二，检查 AC Flash 中瘦 AP 版本文件与 AC 版本文件的上载时间是否一致，如果时间相差超过 1 天，则很有可能版本不匹配，需要重新上传正确的瘦 AP 版本文件至 AC Flash。

命令：*dir*

```
<AC>dir
Directory of cfa0:/

0    -rw-    5441472  May 20 2013 19:16:50   wa2600ae_fit.bin
1    -rw-    6164168  May 20 2013 19:17:18   wa3600_fit.bin
2    -rw-   45386804  May 23 2013 19:21:34   wx6103-cmw520-r2308p14.bin
```

第三，检查 AP 注册状态，如果 AP 状态反复停留在 IL(ImageLoad)无法上线，则很有可能为 AC、AP 版本不匹配，需要重新上传正确的瘦 AP 版本文件至 AC Flash。

命令：*display wlan ap all*

例如：AP 反复停留在 IL 状态，则很有可能为版本文件不匹配。

```
<H3C>display wlan ap all
State :I = Idle,    J = Join, JA = JoinAck,    IL = ImageLoad
        C = Config, R = Run, KU = KeyUpdate, KC = KeyCfm
-------------------------------------------------------------------------------
 AP Name                       State  Model           Serial-ID
-------------------------------------------------------------------------------
 fz_dgl_001                    IL     WA1208E-GP      210235A0A9C094001953
 fz_dgl_002                    IL     WA1208E-GP      210235A0A9C094001529
 fz_dgl_003                    R/M    WA2100          210235A22WB093001434
```

② 检查 AP 模板配置。

命令：*display current-configuration*

例如：检查 AP 型号、序列号配置，确保跟 AP 的真实信息一致。

```
<AC>display current-configuration
 #
wlan apfz_dgl_001 model WA1208E-GP id 76
 priority level 7
 serial-id210235A0A9C094001953
 radio 1
```

另外，如果 AP 通过 MAC 地址信息注册 AC。此时需要确保 AP MAC 地址信息正确。

```
<AC>display current-configuration
 #
wlan apfz_dgl_001 model WA1208E-GP id 76
 priority level 7
 serial-id0023-8999-fec0
 radio 1
```

(11) 检查 AC License

查看 AC License，对比 AC 上 AP 注册数目，确定是否需要 License 扩容。

① 检查 AC License 所支持的 AP 注册数量。

命令：*display license ap*

```
<AC>display license ap
No. Serial number                                AP Number    Available Time Left
------------------------------------------------------------------------------
 1  ZrxbR-5nHmt-$C&tn-acm55-q&qSN-D+:K3-b9EFH     128          Forever
 2  yb@Cc-LNw4c-dYGr9-hxe$r-kr/k4-Cj3s3-@/hcq     128          Forever
 3  uc$tS-wJk3q-rKrc+-$Eq9n-F6inS-+U5&z-2K4gg     128          Forever
```

计算公式：

$$\text{AC 支持的 AP 注册数量} = \text{该型号 AC 默认规格} + \sum \text{每条 License 步长}$$

注意： 当 AC 添加 License 后，需要重启 AC，License 才能生效。

② 检查 AC 当前已经注册的 AP 数量。

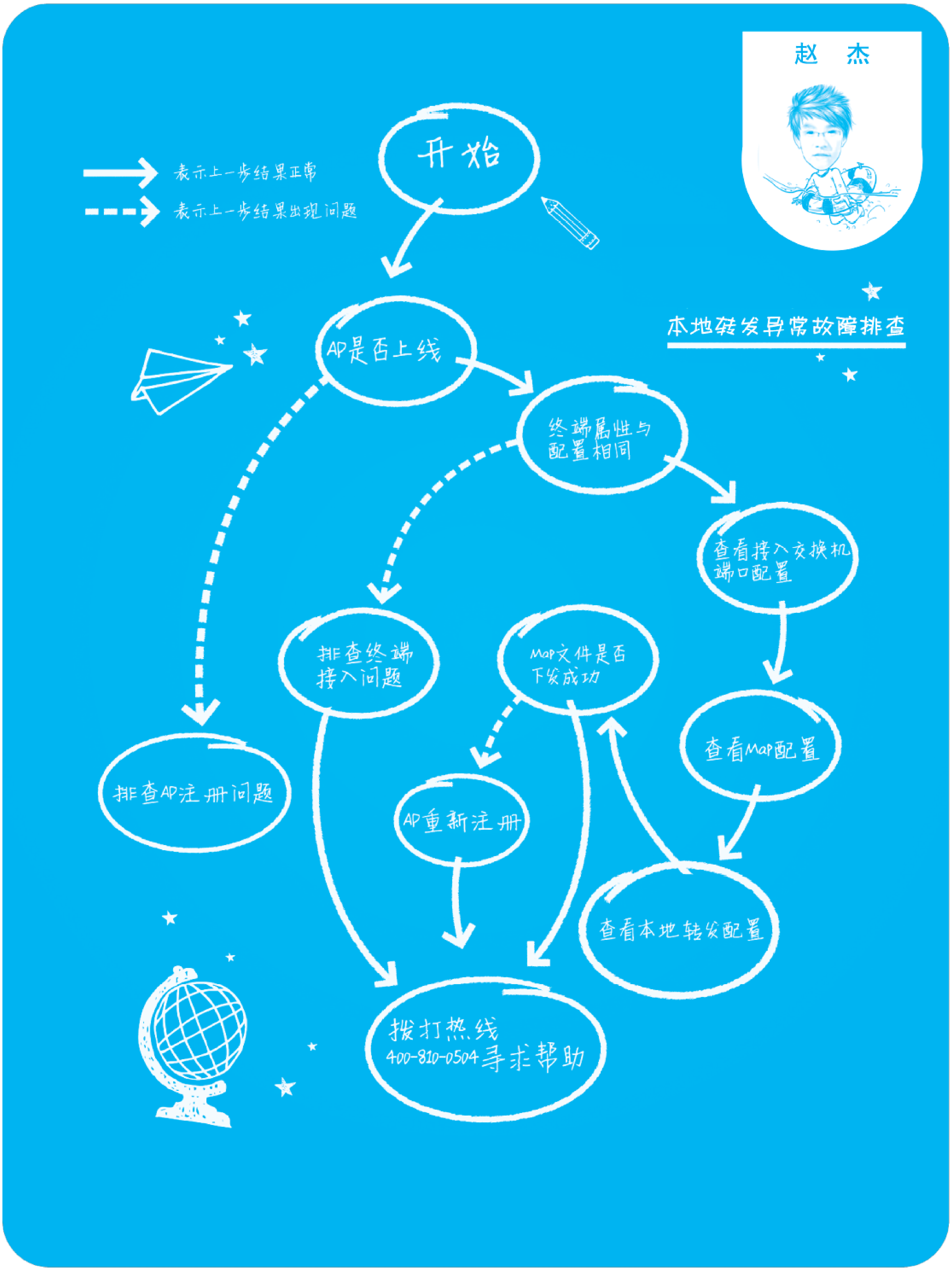
命令：*display wlan ap all*

```
<AC> display wlan ap all
 Total Number of APs configured              : 729
 Total Number of configured APs connected    : 613
 Total Number of auto APs connected          : 0
```

计算公式：

AP 当前注册数量 =“Total Number of configured APs connected”
+“Total Number of auto APs connected”

③ 对比确认是否需要对 License 扩容。比较“AC 支持的 AP 注册数量”和“AP 当前注册数量”，如果二者相等，则说明 AC License 达到允许注册的 AP 数上限，AC 需要 License 扩容。


赵 杰
表示上一步结果正常
表示上一步结果出现问题
本地转发异常故障排查
开始
AP是否上线
终端属性与配置相同
查看接入交换机端口配置
查看Map配置
查看本地转发配置
Map文件是否下发成功
AP重新注册
排查终端接入问题
排查AP注册问题
拨打热线
400-810-0504寻求帮助

1. 开始

无线局域网数据转发模式分为集中式转发和本地转发，集中式转发模式下，数据通过 AC 统一转发；本地转发模式下，数据报文通过接入层交换机转发。本地转发模式问题排查思路。

① 检查 AP 在线情况。

② 检查终端接入属性(SSID 和 VLAN)。

③ 检查接入交换机端口配置。

④ 检查 MAP 文件配置以及是否下发成功。

2. 流程图相关操作说明

(1) AP 是否上线

本地转发基于 AP 稳定注册在 AC 上，排查问题前查看 AP 是否稳定在线。

命令：*display wlan ap xxx verbose*

display version

例如：通过命令查看 AP 在 AC 上注册时长以及 AP 运行时长，如果两个时长相近，说明 AP 稳定注册在 AC，否则需要排查 AP 掉线问题。

① 查看 AP 注册时长。

```
[AC]display wlan ap name ap1 verbose
                              AP Profile: ap1
--------------------------------------------------------------------------------
 APID                                  : 1
State                                  :Run
 Up Time(hh:mm:ss)                     :07:01:34
```

② 查看 AP 运行时长。

```
[WA2620]display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 1304P03
Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C WA2620 uptime is 0 week, 0 day,7 hours, 7 minutes
```

(2) 终端属性与配置相同

无线本地转发是基于 SSID＋VLAN 实现，如果终端接入无线的 SSID 和 VLAN 与配置相同，AP 由本地转发模式传送数据；如果终端接入 SSID 相同，但是 VLAN 不是本地转发 VLAN，数据通过集中式转发传送。

命令：*display wlan client*

display current-configuration configuration wlan-st

例如：通过命令查看接入终端连接的 SSID 以及所属 VLAN。

```
[AC]display wlan client
 Total Number of Clients                    : 2
                                Client Information
```

```
SSID:H3C
-----------------------------------------------------------------------------------------
MAC Address User Name        APID/RID IP Address                    VLAN
-----------------------------------------------------------------------------------------
001e-654c-6708 -NA-            1/2       0.0.0.0                      20
-----------------------------------------------------------------------------------------
```

检查本地转发配置 SSID+VLAN。

```
[AC]display current-configuration configuration wlan-st
#
wlan service-template 1 clear
 ssid H3C
 bind WLAN-ESS 1
 client forwarding-mode local vlan 20
 service-template enable
#
```

（3）查看接入交换机端口配置

交换机为 AP 提供数据转发通道，在本地转发模式下，要求交换机连接 AP 的端口，允许 AP 管理 VLAN 和终端业务 VLAN 通过，端口 PVID 为 AP 管理 VLAN ID。

命令：*display current-configuration interface xxx*

例如：通过命令查看接入交换机端口配置，AP 管理 VLAN 是 10，终端业务 VLAN 是 20，接口 PVID 应该配置为 VLAN 10。

```
[H3C]display current-configuration interface Ethernet 1/0/1
#
interface Ethernet1/0/1
 poe enable
 port link-type trunk
 port trunk permit vlan10 20
 port trunk pvid vlan 10
#
```

（4）查看 MAP 配置

本地转发模式通过 MAP 文件对 AP 下发配置，MAP 文件配置 AP 以太网端口为 Trunk 模式，允许用户业务 VLAN 通过，特殊配置也可以通过 MAP 文件下发。MAP 文件是一个 txt 文件，编辑 txt 文件输入 AP 上需要配置的命令，默认情况下在系统视图（说明：[AP]），将编辑好的 MAP 文件上传到 AC Flash→CF 卡中，通过命令给 AP 指定 MAP 文件下发。

命令：*more map.txt*

例如：通过命令查看 AC Flash→CF 卡中的 MAP 文件。

```
<AC>more map.txt
interface Ethernet1/0/1
port link-type trunk
port trunk  permit vlan 20
```

说明： 802.11g AP 以太网口是百兆口，802.11n AP 以太网口是千兆口，如果 MAP 文件编写错误，命令将下发失败，MAP 文件内不要有空格等多余字符。

（5）MAP文件是否下发成功

MAP文件内容下发到AP，等同于手动在AP上配置命令，因此可以远程Telnet到AP上查看配置来确定MAP文件是否下发成功。

命令：*display current-configuration interface Ethernet XXX*

例如：Telnet到AP上查看配置是否下发成功。

```
<AP> display current-configuration interface Ethernet 1/0/1
#
interfaceEthernet1/0/1
port link-type trunk
port trunk   permit vlan10 20
#
```

（6）排查AP注册问题

排查AP注册问题请参考云图工程《瘦AP注册不上故障排查》。

（7）排查终端接入问题

排查终端接入SSID与VLAN，连接SSID由终端控制，接入VLAN由设备和认证服务器控制。如果SSID有认证且通过认证服务器下发VLAN，那么需要查看服务器下发VLAN属性；如果没有认证或者认证未涉及下发VLAN，则接入VLAN在设备上控制，无线设备可以通过ESS接口或者AP绑定服务下发VLAN。

命令：*display current-configuration interface wlan-ess xx*

display current-configuration configuration wlan-ap

例如：查看无线接口接入权限。

```
[AC]display current-configuration interface WLAN-ESS 2
interface WLAN-ESS2
 port link-type   hybrid
 port hybrid pvid vlan 2
```

查看基于AP控制终端接入权限。

```
[AC]display current-configuration configuration wlan-ap
wlan ap ap1 model WA2620 id 1
 serial-id 219801A0D1C123023703
 radio 1
 radio 2
  service-template 1 vlan-id 20
  radio enable
```

终端接入权限控制优先级：认证服务器下发权限→基于AP控制权限→基于无线接口控制权限。

（8）AP重新注册

本地转发配置文件上传到AC Flash→CF卡，并在AP模版下指定下发配置文件，未上线AP在注册成功后会自动下发MAP文件，如果AP已经上线，需要重新注册下发MAP文件，AP重新注册可以断开AP有线网络，或者重启AP。

命令：*reset wlan ap name xxx*

例如：通过命令让AP重启并重新注册。

```
<AC>reset wlan ap name ap1
 This command will reset only master connection AP.
 Do you want to continue [Y/N]:Y
```

(9) 查看本地转发配置

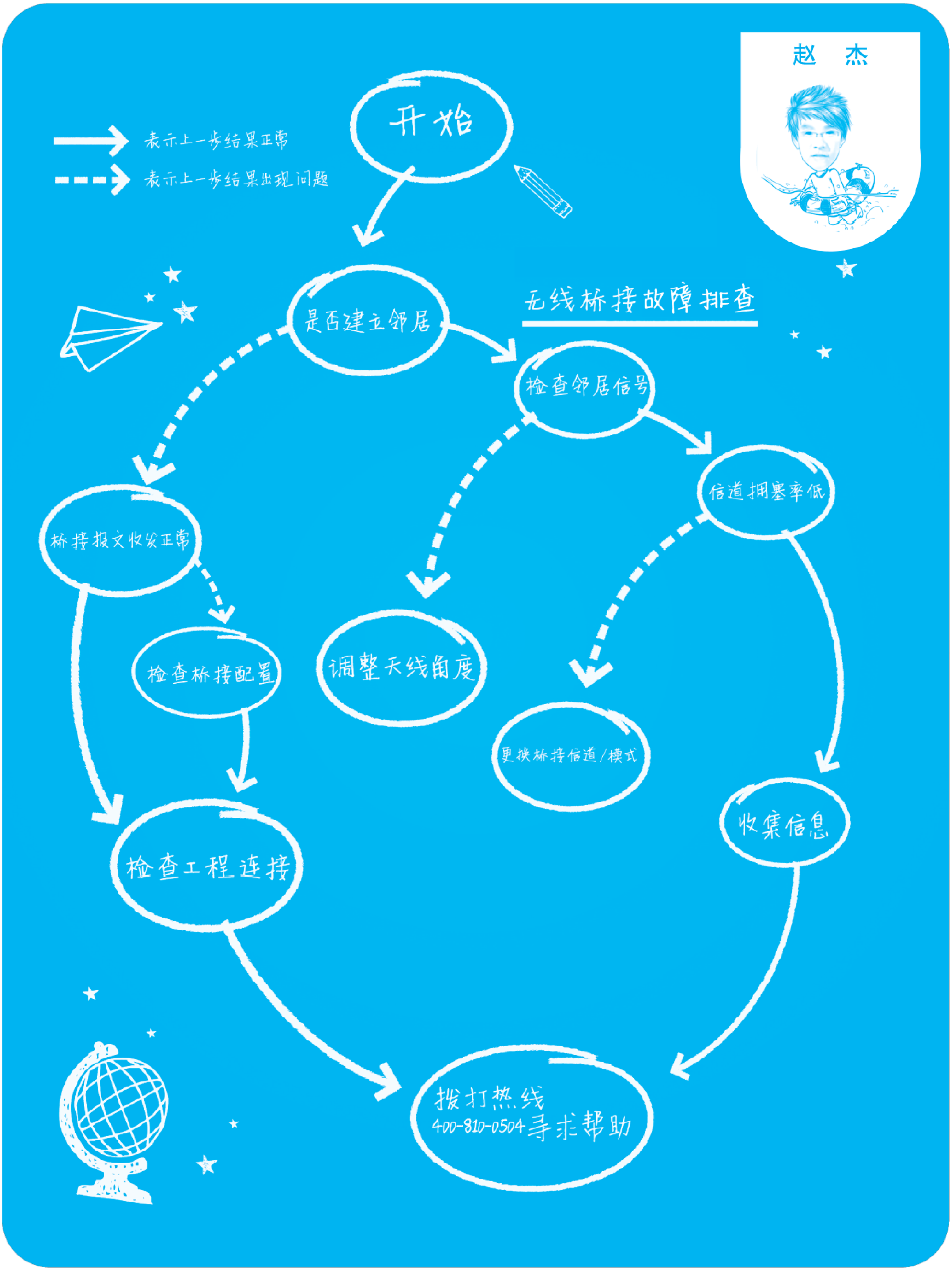
本地转发基于 SSID+VLAN,重点注意 SSID 与 VLAN 的绑定关系,同时注意 AP 绑定的 MAP 文件。

命令: *display current-configuration configuration wlan-ap*

display current-configuration configuration wlan-st

```
[AC]display current-configuration configuration wlan-ap
#
wlan ap ap1 model WA2620 id 1
map-configuration map.txt
 priority level 7
 serial-id 219801A0D1C123023703
 radio 1
 radio 2
  service-template1
  radio enable
```

```
[AC]display current-configuration configuration wlan-st
#
wlan service-template 1 clear
 ssid H3C
 bind WLAN-ESS 1
 client forwarding-mode local vlan 20
 service-template enable
#
```


赵 杰
开始
表示上一步结果正常
表示上一步结果出现问题
是否建立邻居
无线桥接故障排查
检查邻居信号
信道拥塞率低
桥接报文收发正常
检查桥接配置
调整天线角度
更换桥接信道/模式
收集信息
检查工程连接
拨打热线
400-810-0504寻求帮助

1. 开始

无线桥接(MESH 技术)又称为 WDS 链路,无线桥接链路质量与工程连接、设备配置、无线信道质量有关,桥接问题定位思路:先排查工程连接,再排查无线桥接信号,最后排查无线信道质量。建议工程安装前测试桥接链路,确保桥接配置、器件质量没问题。

2. 流程图相关操作说明

(1) 是否建立邻居

桥接链路是两个 AP 之间建立 MESH 链路,桥接链路建立成功后,设备能够看到邻居 MAC 地址、MESH 信号强度以及邻居状态为 Active。

命令:*display wlan mesh-link all*

例如:在设备上查看邻居链路信息,如果没有建立邻居,则返回值为空。

```
[AP]display wlan mesh-link all
                              Peer Link Information
-----------------------------------------------------------------------------------------
 Nbr-Mac(rssi)      BSSID            Interface          Link-state   Uptime(hh:mm:ss)
-----------------------------------------------------------------------------------------
5866-ba64-61e0(48) 5866-ba64-a210 WLAN-MESHLINK113    Active            0: 0: 6
-----------------------------------------------------------------------------------------
```

(2) 检查邻居信号

为了保证链路通信质量,邻居信号要求大于 30(RSSI>30),如果已经建立链路,但是信号比较弱,可以调整 AP 发射功率、天线方位角/下倾角改善邻居信号。

命令:*display wlan mesh neighbors all*

例如:通过命令查看邻居详细信息,Mean RSSI 是设备收到邻居的信号强度,为了保证链路质量,要求信号强度大于 30。

```
[AP] _hidecmd
[AP-hidecmd]display wlan mesh neighbors all
                                   Mesh Neighbor Parameters
-----------------------------------------------------------------------------------------
 Neighbor MINDEX                    :1280
 BSS ID                             :5866-ba64-a210
 Peer Mac Addr                      :5866-ba64-61e0
 Mesh ID                            :H3C
 Neighbor state                     :Connected peer
 Mean RSSI                          :48
 Zero Config State                  :No
-----------------------------------------------------------------------------------------
 Link FSM State                     :Established
 Peer's LinkId                      :0001
 Interface Index                    :00CC0000
-----------------------------------------------------------------------------------------
```

(3) 信道拥塞率低

桥接链路使用固定信道，桥接两端设备通过信道交互保活报文和数据报文，如果信道拥塞，保活报文被丢弃，桥接链路可能频繁断开重连。

命令：*display ar5drv 2 channelbusy*

例如：通过命令查看信道拥塞情况，在没有业务流量的情况时，如果信道质量较差，CtlBusy 数值大于 30%，建议更换信道或者频段，使用信道质量相对较好的信道。

```
[AP-hidecmd]display ar5drv 2 channelbusy
ChannelBusy information
 Ctl Channel:      11      Channel Band: 20M
 Ext Channel:
 Record Interval(s):   9
 Date/Month/Year: 17/11/2011
         Time(h/m/s):  CtlBusy(%) TxBusy(%)   RxBusy(%)   ExtBusy(%)
 01      21:57:37         64          1           56           0
 02      21:57:28         64          1           56           0
```

(4) 桥接报文收发正常

桥接设备通过 Beacon 帧发送桥接建立请求，同时设备实时的扫描接收对端发送的 Beacon 帧，连续多次查看设备收发 Beacon 帧统计，正常情况收发帧统计应该持续增加，统计数据可以辅助判断两端设备工作是否正常。BeaconIntCnt 记录本端设备 Beacon 发送数量，如果连续多次收集没有持续增加，需要排查本端桥接配置；RxFrameCnt 记录收到邻居设备帧数量，如果连续多次收集没有持续增加，需要检查邻居设备配置以及两端工程连接。

命令：*display ar5drv 2 statistics*

例如：在连续多次在设备上收集统计信息，查看设备收发报文统计是否持续增长。

```
[AP-hidecmd]display ar5drv 2 statistics
Radio statistics:
 TxFrameAllCnt          : 1649
 TxFrameAllBytes        : 295811
--------------------------------------------
Management statistics
 ProbeRespSuc           : 561
 ProbeRespFail          : 20
 OutputErrs             : 2
 RtsSuccessCnt          : 0
 TxFilteredCnt          : 0
 TxHwRetryExcesive      : 22
 TxSwRetryExcesive      : 0
 SwRetryCheckFail       : 0
 RxFrameAllCnt          : 2470717
 RxFrameCnt             : 13372
 RxFrameBytes           : 1853985
 InputErrs              : 749030
 RadioResetOnErr        : 0
 RadioResetTxDone       : 0

Beacon statistics
 BeaconIntCnt           : 6969
 BeaconBusyCnt          : 0
 BeaconErrCnt           : 0
```

（5）调整天线角度

天线方位角和下倾角共同决定天线主波瓣方向，桥接链路要求两端天线主波瓣方向尽可能重叠，同时天线极化方向需要一致。在链路已经建立但是信号较弱，或者可以收到对端报文没有建立链路情况下，先固定一端天线角度，左右调整另一端天线方位角，或者上下调整下倾角，增加两边天线主波瓣重叠度，达到优化桥接信号的目的，如图 7-24 所示。



图 7-24　调整天线角度

（6）更改桥接信道/模式

桥接通信之前测试信道带宽利用情况，如果信道带宽占用比例较大，说明该信道干扰相对较大，建议更改桥接信道，选用信道质量相对较好的信道作为桥接使用，必要时可以更换工作频段。

命令：*radio-type dot11g*

　　　channel 11

例如：更改 AP 射频工作模式为 802.11g，更改 AP 工作信道为 11。

```
[AP]interface WLAN-Radio1/0/1
[AP-WLAN-Radio1/0/1]radio-type dot11g
[AP-WLAN-Radio1/0/1]channel 11
```

（7）检查桥接配置

设备收发报文统计为 0 或者没有持续增加，如果 BeaconIntCnt 计数没有增加，则检查本端配置，如果 RxFrameCnt 计数没有增加，则检查对端配置。

① 检查端口安全配置。

```
[AP]port-security enable
```

② 检查 MESH 接口配置，两个设备 MESH 下配置必须一致，同时接口 pvid 必须是已定义的 VLAN。

```
[AP]display current-configuration interface WLAN-MESH 1
#
interface WLAN-MESH1
port link-type trunk
 port trunk permit vlan all
 port-security port-mode psk
 port-security tx-key-type 11key
 port-security preshared-key pass-phrase cipher
$ c $ 3 $ Vl4iKUOrwhwD3RSlu63RhNMOBTRE7Mi1YhAg
```

③ 检查 mesh-profile 配置，两端 mesh-id 必须配置一致，否则无法建立链路。

```
[AP]display wlan mesh-profile 1
-----------------------------------------------------------------------------
 Mesh Profile Number                          : 1
 Mesh ID                                      :H3C
 Binding Interface                            : WLAN-MESH1
 Link Keep Alive Interval (s)                 : 2 (Default)
 Link Backhaul Rate (Mbps)                    : 18 (Default)
 Mesh Profile Status                          : Disable
-----------------------------------------------------------------------------
```

④ 检查射频口配置，两个设备工作协议、信道必须一致，如果绑定 Peer-Mac，MAC 地址必须是对端 MESH Radio 的 MAC。

```
[AP] dis current-configuration interface   WLAN-Radio 1/0/2
#
interface WLAN-Radio1/0/2
 radio-typedot11g
 channel 11
 mesh-profile 1
 mesh peer-mac-address 5866-ba64-61e0
#
```

(8) 检查工程连接

工程检查需要确认 AP 与馈线、馈线与天线、网线等连接情况，可以根据下面顺序排查。

① 确认 AP 是否正常启动，可以通过 Console 口登录或者面板指示灯确认。

② 确认桥接链路工作信道。

③ 检查 AP 协议馈线口与天线协议馈线口连接是否正确紧密。

④ 检查 AP 与天线极化连接方式，对于双流两个馈线口的 AP 需要分别连接天线水平和垂直极化方向；对于双流三个馈线口的 AP，AP 馈线口 1 和 3 分别连接天线水平和垂直极化方向(WA2610E-AGN 和 WA2620E-AGN 除外，连接方式参考天线连接指导)，对于三流三馈线口的 AP，按顺序连接天线馈线口。

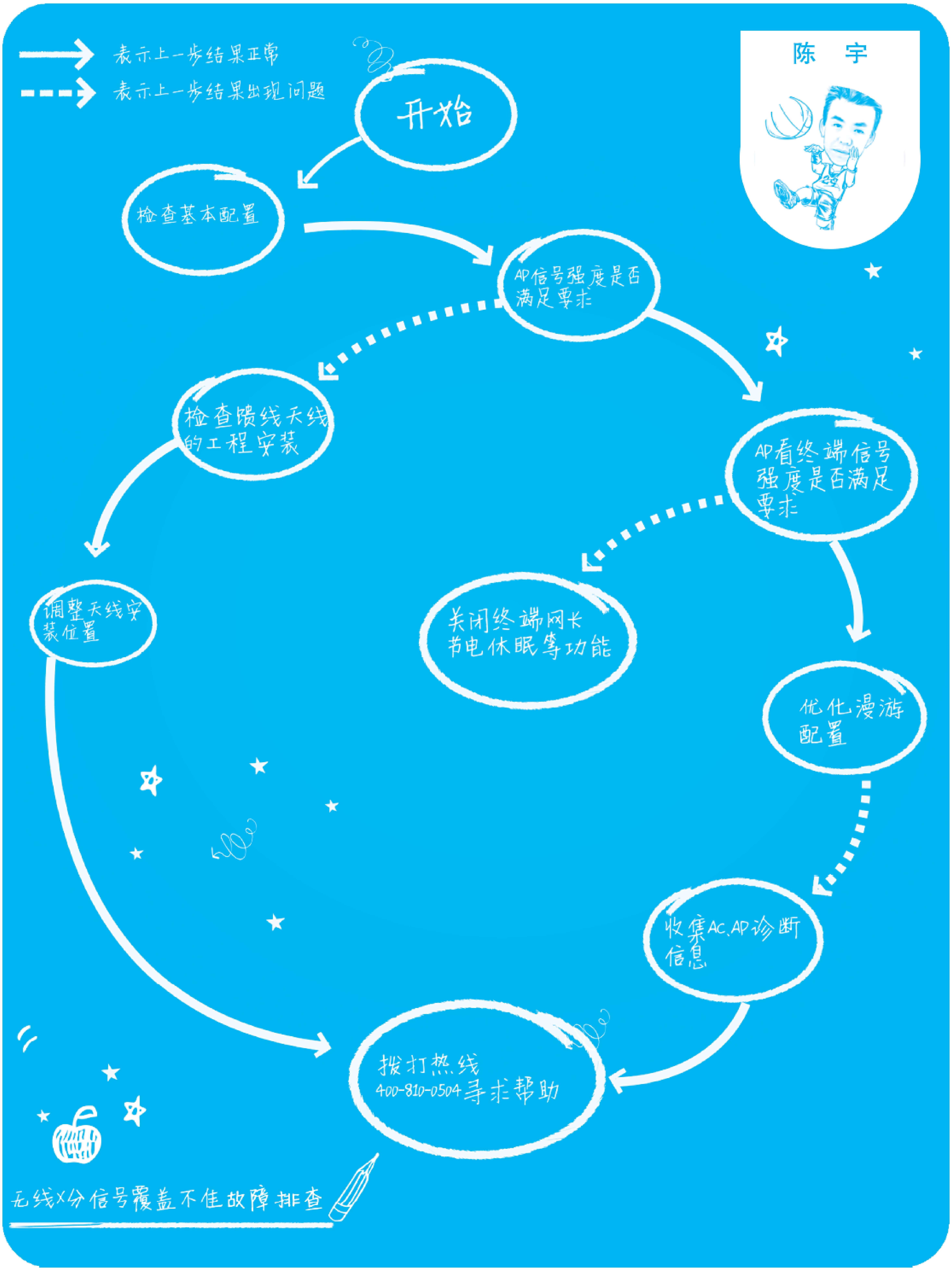
⑤ 检查网线馈线防水防尘处理，室外 AP 做好接地、防雷处理。

⑥ 检查桥接两侧天线主波瓣方向是否对准。

(9) 收集信息

通过以上步骤分析依旧无法解决问题，收集以下信息反馈 H3C 售后技术人员分析处理。

```
<H3C>display current-configuration
<H3C>debugging wlan mesh all
<H3C>debugging port-security all
<H3C>terminal debugging
<H3C>terminal debugging
```



表示上一步结果正常
表示上一步结果出现问题
陈 宇
开始
检查基本配置
AP信号强度是否满足要求
检查馈线天线的工程安装
调整天线安装位置
AP看终端信号强度是否满足要求
关闭终端网卡节电休眠等功能
优化漫游配置
收集AC、AP诊断信息
拨打热线 400-810-0504寻求帮助
无线X分信号覆盖不佳故障排查

07 无线产品 > 7.2 AP > 7.2.4 无线 X 分信号覆盖不佳故障排查 > 步骤详解

1. 开始

无线 X 分覆盖方案主要应用于医院等场景。X 分信号覆盖的好坏与工程连接、设备配置、终端网卡等都有关系。X 分信号覆盖不佳问题定位思路：先明确故障现象，再排查设备配置、工程连接，最后排查 AP、终端信号强度等问题。

2. 流程图相关操作说明

（1）检查基本配置

检查 AC 的基本配置，排查 X 分信号覆盖不佳是否由于功率、国家码配置错误导致。一般情况下，无线 X 分覆盖方案相关中 AP 都配置为最大功率，即 max-power 配置为最大值（不同型号 AP 存在差异）。另外，设备上国家码的配置有可能导致 AP 的默认最大发射功率发生变化（如 Au 国家码的 802.11a 默认 max-power 为 12），因此必须保证所有 AP 采用最大功率发射并且国家码 country-code 配置为 CN。

此外，X 分 AP 的静谧工作模式在某些情况下也有可能被误判为信号覆盖不佳，因此在排查信号覆盖的时候，建议如果开启静谧模式可以先关闭此功能。

命令：*display wlan ap name xxx radio*

display wlan country-code ap all

max-power xxx

wlan country-code CN

undo wlan option x-share quiet enable

例如：通过命令查看 AP 的功率配置和国家码，并且修改功率和关闭静谧工作模式，如下所示。

```
[WX6108-AC]display wlan ap name ap1 radio
                              AP Radio
--------------------------------------------------------------------------------
 AP Name                       Radio ID        Channel        Tx Power (dBm)
--------------------------------------------------------------------------------
 ap1                              1            auto               20
 ap1                              2            auto               15
--------------------------------------------------------------------------------
[WX6108-AC]wlan ap ap1
[WX6108-AC-wlan-ap-ap1]radio 2
[WX6108-AC-wlan-ap-ap1-radio-2]max-power ?
  INTEGER<1-20>   Specify maximum radio power in dBm (Default: 20)
[WX6108-AC-wlan-ap-ap1-radio-2]max-power 20
[WX6108-AC]wlan country-code CN
 This command will disable the radio and reset the radio parameters.
 Do you want to continue? [Y/N]Y
[WX6108-AC]display wlan country-code ap all
                            Country Code
--------------------------------------------------------------------------------
 AP                                    Country Code
--------------------------------------------------------------------------------
```

```
ap1                                   CN   CHINA
ap2                                   CN   CHINA
ap3                                   CN   CHINA
[WX6108-AC]display current-configuration | include option
 option 43 hex 800F0000 03A00100 64A00100 04A00100 36
 wlan option fair-schedule enable
 wlan option traffic-shaping enable
 wlan option client-reject 15
 wlan option tpc enable
 wlan option x-share quiet enable
[WX6108-AC]undo wlan option x-share quiet enable
```

(2) AP 信号强度是否满足要求

在终端上查看 AP 实际的信号强度。为了保证业务的正常应用，X 分覆盖场景下，PC 终端要求 AP 信号强度≥－70dBm，智能终端（手机、PDA、平板等）要求 AP 信号强度≥－65dBm。一般推荐 PC 端可选的软件如 NetStumbler（只能在 XP 系统使用）、WirelessMon、inSSIDer，智能终端可选软件如 Wi-Fi 分析仪等，inSSIDer 在终端查看 AP 信号强度如图 7-25 所示。

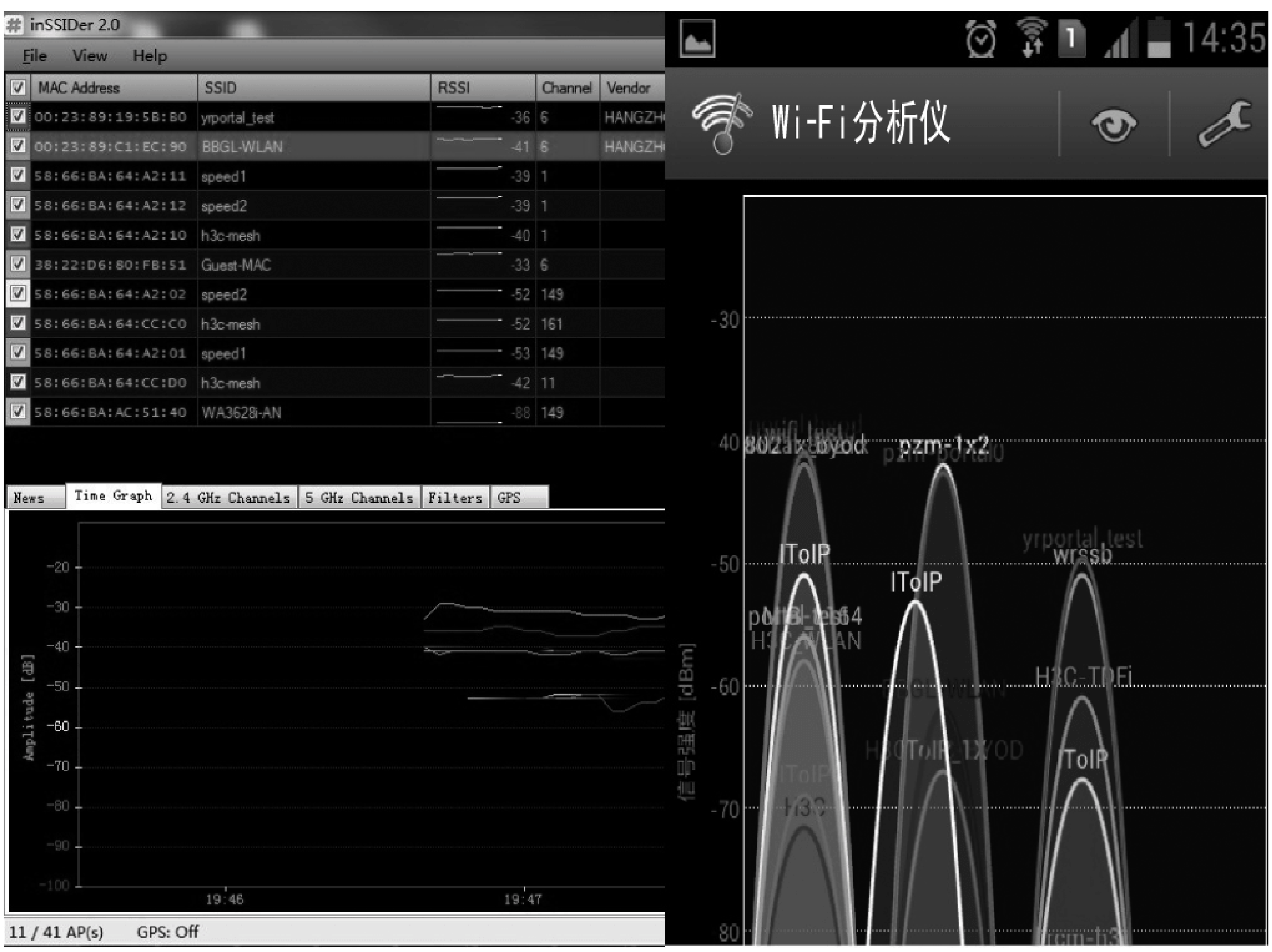


图 7-25 inSSIDer 在终端查看 AP 实际的信号强度

(3) 检查馈线天线的工程安装

关于馈线、天线的工程安装问题，主要包含以下几个方面。

① 必须保证所有的接口拧紧、无滑丝或者松动，对于未接馈线的天馈口需要用负载堵住。

② 一般情况下，馈线的长度建议不超过 10m。另外，馈线材质不同线损也不一样，实际

测试时需要兼顾考虑,必要时可以替换线损较小的材质馈线替换测试信号强度。

③ 如果用同一个终端在相同距离下测试同一个 AP 不同天馈的信号强度存在明显差异(一般 10dBm 以上),而所采用的馈线材质和长度、天线型号都一样,则要求进行馈线、天线的替换测试,确认是 AP 本身问题还是天馈线质量问题。

④ 对于 X 分 AP,需要按照安装指导规范连接天线和 AP 馈线口。图 7-26 所示为 6 个房间覆盖的示意图。

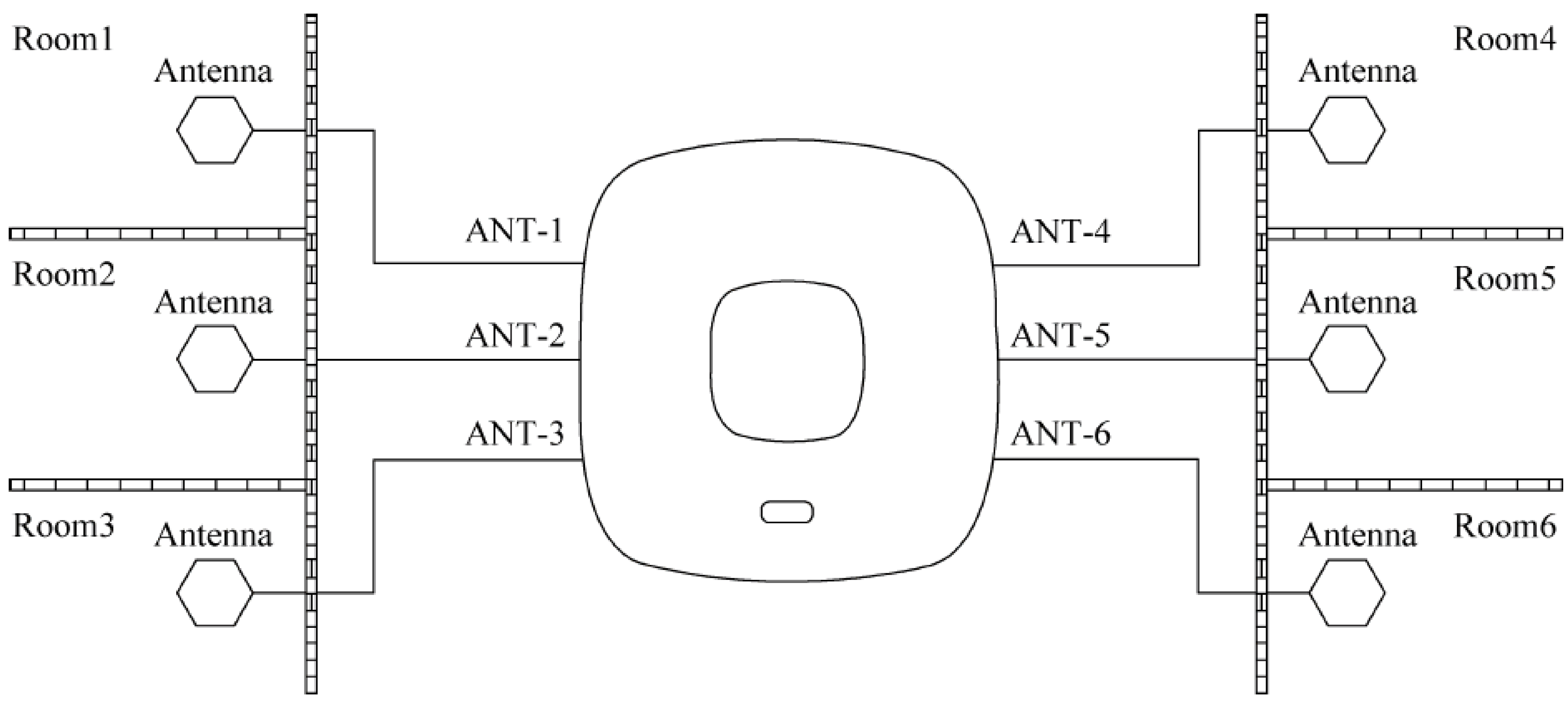


图 7-26　6 个房间覆盖的示意图

(4) 调整天线安装位置

如果测试发现仍存在信号覆盖不佳问题,通过替换天线、馈线无法改善,可以调整天线的安装位置或者增加 AP 补充覆盖,保证边缘区域的信号强度。需要注意的是,当增加 AP 时,必须重新规划整层楼、跨楼层间的所有 AP 信道部署,减少干扰。

(5) 看 AP 终端信号强度是否满足要求

如果 AP 上看到终端的 RSSI<25,且协商速率 Rx 方向数值较低,说明可能是由于终端自身网卡功率过低造成的。由于之前已经排除了 AP 故障的可能,这时需要考虑是否网卡本身原因导致 RSSI 和协商速率较低。

测试方法:可选择在一个天线正下方测试,另外可以更换成 PC 或其他终端对比测试,看看是普遍存在的问题还是个别问题。一般来说,PC 终端的网卡功率略高于智能终端(手机、PDA、平板等)。

命令:*display wlan client verbose*

例如:在 AC 上通过命令查看终端关联信息,RSSI 为 19,Rx/Tx 协商速率为 1/48,该终端发射信号功率可能偏弱。

```
<WX5540E>display wlan client verbose
 Total Number of Clients           : 8
 TotalNumber of Clients Connected : 8
                              Client Information
------------------------------------------------------------------------
 MAC Address                       : 0018-ded7-7b47
 AID                               : 251
 AP Name                           : 129
 Radio Id                          : 1
```

```
SSID                                       : user_wlan
 BSSID                                     : 0023-899f-5312
 Port                                      : WLAN-DBSS4:702
 VLAN                                      : 613
 State                                     : Running
 PowerSave Mode                            : Active
 Wireless Mode                             : 11g
 QoS Mode                                  : WMM
 Listen Interval (Beacon Interval)         : 10
 RSSI                                      : 19
 Rx/Tx Rate                                : 1/48
 Client Type                               : PRE-RSNA
 Authentication Method                     : Open System
 AKM Method                                : None
 4-Way Handshake State                     : -NA-
 Group Key State                           : -NA-
 Encryption Cipher                         : Clear
 Roam Status                               : Intra-ACroam association
 Up Time (hh:mm:ss)                        : 01:00:27
-----------------------------------------------------------------------------
```

(6) 关闭终端网卡节电休眠等功能

部分终端的网卡设置中默认开启了网卡节电等功能，由于 X 分覆盖场景的特殊需求，我们需要调整终端设置保证业务应用。PC 终端、医疗专用 PDA 终端等都可以设置节电和休眠功能。下面以 Windows 7 系统的 PC 为例，可按“控制面板→网络与共享中心→更改适配器设置→无线网络连接→右击‘属性’→网络→配置”的路径进行设置，如图 7-27 所示。



图 7-27 Windows 7 系统的 PC 设置

如图 7-27 所示，“传输电源”选择为“最高值”表示笔记本网卡工作在最大功率状态，否则有可能造成网卡性能降低；“允许计算机关闭此设备以节约电源”不勾选表示关闭网卡的节电

模式。

(7) 优化漫游配置

如果通过以上几步仍无法解决问题，那么就需要关注信号不佳问题是否是漫游效果不佳导致的。如果信号覆盖不佳的问题只出现在两个 AP 间的覆盖区域时，这时候很有可能就是终端漫游性能较差导致的。由于之前已经排查过工程安装和天线位置等因素，因此这里我们可以通过 AC 的配置优化引导漫游性能较差的终端主动发生漫游。这里的优化命令主要包含以下 3 个。

命令 1：*wlan option roam-navigation level xx xx x*

解释：开启漫游导航功能，3 个参数分别表示全局漫游导航级别、终端信号强度门限和终端漫游导航级别，建议配置为 10 25 1，其中门限值可根据现场业务实际测试效果配置在 25±5 的取值范围内。

命令 2：*wlan option client-reconnect-trigger xxx signal-check*

解释：主动触发客户端重关联功能，参数表示功能触发的终端信号强度门限值，建议配置为 20，同样可以根据现场业务实际测试效果配置为 20±5。

命令 3：*wlan option client-reject xxx*

解释：禁止弱信号终端接入功能，参数表示允许接入的客户端最小信号强度的门限值，建议配置为 15，可根据现场业务实际测试效果配置为 15±5。

需要注意的是，上述三条命令开启后，需要整体测试业务情况，特别是主动触发客户端重关联和禁止弱信号终端接入功能开启后，某些智能终端的重关联过程可能伴随有丢包情况，这时对丢包比较敏感的业务（如远程桌面等）可能会中断。总而言之，漫游是终端自身的行为，WLAN 设备只能尽量引导终端合理地去漫游，上述命令需要反复调测得出匹配业务场景的最佳参数。

(8) 收集 AC、AP 诊断信息

通过以上步骤分析依旧无法解决问题，请收集 AC 和问题 AP 的诊断信息，反馈 H3C 售后技术工程师分析。

命令：*display diagnostic-information*



赵 杰
表示上一步结果正常
表示上一步结果出现问题
开始
单播ping丢包是否连续
检查业务流量是否拥塞
存在主链路异常切换日志
主链路信号强度大于30
备份链路信号强度大于主链路
信道利用率是否正常
优化主链路保持时间参数,减少频繁切换
优化切换信号阈值
检查有线设备转发表项
排除干扰
检查MR配置
检查轨旁AP
检查mlsp-proxy参数
检查AC配置
拨打热线 400-810-0504寻求帮助
无线桥接快速切换故障排查

1. 开始

无线桥接组网使用 MESH 技术，在 PIS、CBTC 等特殊应用场景下，车载 MR 快速移动并依次与轨旁 AP 进行 MESH 链路切换。为保证链路稳定性，MESH 链路维护需遵循以下原则：MESH 主链路信号强、信道利用率低、链路切换参数合理。

常见桥接应用设备定义。

移动桥接设备：车载 MR。

固定桥接设备：轨旁 AP。

2. 流程图相关操作说明

(1) 单播 ping 丢包是否连续

不带业务 ping 测试。在核心交换机下联一个测试服务器，在车载 MR 侧直连或者车载交换机下联测试 PC，测试 PC 上使用 ping 软件(如 Fping)ping 测试服务器 IP 地址，设置 ping 发包间隔为 10ms。车载 MR 从起始点运行到终点，测试结束查看 ping 结果，如果连续丢包超过 5 个，定义为连续丢包，否则可认为链路正常。

例如：实际测试数据，某一时刻连续丢包 8 个，存在异常。

```
61 12/30 02:03:17.843 TooLate #335 Reply 32 bytes from 10.68.92.1: time=37ms TTL=255, ave=
14.00ms
62 12/30 02:03:18.093 TimeOut #336 ***** (32 bytes) Request timed out.
63 12/30 02:03:18.593 TimeOut #337 ***** (32 bytes) Request timed out.
64 12/30 02:03:19.093 TimeOut #338 ***** (32 bytes) Request timed out.
65 12/30 02:03:19.593 TimeOut #339 ***** (32 bytes) Request timed out.
66 12/30 02:03:20.093 TimeOut #340 ***** (32 bytes) Request timed out.
67 12/30 02:03:20.593 TimeOut #341 ***** (32 bytes) Request timed out.
68 12/30 02:03:21.093 TimeOut #342 ***** (32 bytes) Request timed out.
69 12/30 02:03:21.593 TimeOut #343 ***** (32 bytes) Request timed out.
70 12/30 02:03:21.687 TooLate #344 Reply 32 bytes from 10.68.92.1: time=81ms TTL=255, ave=
14.21ms
```

(2) 存在主链路异常切换日志

车载 MR 在移动过程中，持续与轨旁 AP 进行 MESH 链路切换，主链路切换时会生成切换日志，切换日志记录有 MESH 链路切换前后主链路(轨旁 AP)的 MAC 地址、信号强度、切换时间以及切换原因码，如果切换原因码为 Reason 3，可以判断 MESH 切换存在异常。

命令：*terminal logging*

terminal monitor

例如：通过命令收集 MESH 链路切换日志，分析日志中的原因码信息，原因码释义如下。

Reason 1：首次建立链路。

Reason 2：链路正常切换。

Reason 3：链路异常切换，主链路信号弱、切换频繁、信道利用率异常均会异常切换。

```
%Dec 30 02:28:55:980 2012 Train425-H3C-WA2220E-2 WMSH/6/WMESH_SWITCH_ACTIVE_
LINK: Switch an
active link from 0000-0000 (0)to 0023-89a7-46e0(23) for reason 1 with 11 neighbors and 1 links.
%Dec 30 02:29:08:633 2012 Train425-H3C-WA2220E-2 WMSH/6/WMESH_SWITCH_ACTIVE_
LINK: Switch an
active link from 0023-89a7-46e0 (27)to 0023-89a7-4680(36) for reason 2 with 11 neighbors and 3 links.
%Dec 30 02:29:17:878 2012 Train425-H3C-WA2220E-2 WMSH/6/WMESH_SWITCH_ACTIVE_
LINK: Switch an
active link from 0023-89a7-5e60 (20)to 0023-89de-ab40(33) for reason 3 with 12 neighbors and 3 links.
```

（3）主链路信号强度大于30

车载MR同时与多个轨旁AP建立链路，其中一条为主链路负责转发数据，其余链路为备份链路。当主链路信号强度下降且满足切换条件时，备份链路切换为主链路，主链路信号强度与通信质量强弱相关，要求主链路信号大于30(RSSI>30)。主链路信号低于正常数值，链路存在丢包风险。Link-state标识为Active的链路为主链路。

命令：*display clock*

display wlan mesh-link all

例如：列车运行过程中，每隔2秒使用命令采集主链路信号(可以使用CRT软件执行脚本采集)。

```
<MR>display clock
02:26:13 UTC Sun 12/30/2012
<MR>display wlan mesh-link all
                                   Peer Link Information
---------------------------------------------------------------------------------------
 Nbr-Mac(rssi)     BSSID          Interface          Link-state  Uptime(hh:mm:ss)
---------------------------------------------------------------------------------------
 3822-d6cd-e350(39) 3822-d61e-0bb0 WLAN-MESHLINK266    Active        0: 0:20
 c4ca-d908-cbd0(31) 3822-d61e-0bb0 WLAN-MESHLINK267    Dormant       0: 0: 6
 c4ca-d908-cd70(27) 3822-d61e-0bb0 WLAN-MESHLINK264    Dormant       0: 0:33
---------------------------------------------------------------------------------------
```

（4）检查业务流量是否拥塞

桥接MESH链路的带宽有限，实际业务流量应小于MESH链路带宽，检查当前业务流量带宽，如果实际业务流量接近或者大于MESH链路带宽，联系客户减小和优化业务流量。MESH链路带宽标准如下。

2.4G频段MESH链路带宽：802.11g带宽为15Mbps，802.11n 20MHz带宽为30Mbps。

5.8G频段MESH链路带宽：802.11a带宽为15Mbps，802.11n 40MHz带宽为110Mbps。

（5）信道利用率是否正常

MESH链路使用固定信道，桥接两端设备通过该信道交互保活报文和数据报文。如果信道拥塞，将影响数据业务转发，严重时将影响MESH链路稳定性。

命令：*display ar5drv 2 channelbusy*

例如：通过命令查看车载MR信道利用率，在没有业务流量的情况时，如果信道质量较差，CtlBusy数值大于30%，可以确定为存在外界干扰，业务运行前要求排除外界干扰源，如果无法排除干扰源建议更换信道或者频段，使用空口利用率低的信道。

```
[MR]_hidecmd
[MR-hidecmd]display ar5drv 2 channelbusy
ChannelBusy information
 Ctl Channel:      11      Channel Band: 20M
 Ext Channel:
 Record Interval(s):   9
 Date/Month/Year: 17/11/2011
        Time(h/m/s):  CtlBusy(%) TxBusy(%)  RxBusy(%)  ExtBusy(%)
 01      21:57:37          64          1          56          0
 02      21:57:28          64          1          56          0
```

（6）备份链路信号强度大于主链路

正常情况下，车载 MR 会和多个轨旁 AP 建立桥接链路，其中一条链路为主链路转发数据报文。当主链路达到保持时间且主备份链路信号差值大于配置的阈值时，备份链路切换为主链路。如果信号切换阈值设置不合理，将出现备份链路信号大于主链路信号，影响主备链路平滑切换。

命令：*display wlan mesh-link all*

例如：查看动态测试主备链路信号记录日志，确定是否存在备份链路信号强于主链路信号，但信号差值小于设定阈值(比如 link-switch-margin 设置为 10)。

```
<MR>display wlan mesh-link all
                              Peer Link Information
------------------------------------------------------------------------------------
 Nbr-Mac(rssi)     BSSID          Interface        Link-state   Uptime(hh:mm:ss)
------------------------------------------------------------------------------------
3822-d6cd-e350(24) 3822-d61e-0bb0 WLAN-MESHLINK266  Active         0: 0:20
 c4ca-d908-cbd0(22) 3822-d61e-0bb0 WLAN-MESHLINK267 Dormant        0: 0: 6
 c4ca-d908-cd70(31) 3822-d61e-0bb0 WLAN-MESHLINK264 Dormant        0: 0:33
------------------------------------------------------------------------------------
```

（7）检查有线设备转发表项

了解桥接网络传送报文类型，确定车载 MR 运动过程，轨旁 AP 上行设备转发表项能够及时更新，常见的业务报文包括单播和组播，业务报文为单播报文时，检查轨旁 AP 上行设备的 MAC 表项；业务报文为组播时，检查轨旁 AP 上行设备的组播表项。

命令：*display igmp-snooping group vlan xxx verbose*

display mac-address

① 车载 AP 主链路切换时，轨旁 AP 上行设备应及时更新 MAC 表项，使用命令检查轨旁 AP 上行设备的 MAC 表项是否及时更新。

命令：*display mac-address*

例如：查看轨旁 AP 上行交换机 MAC 地址表项，查看主备链路切换后是否及时更新表项。

```
[S75E] display mac-address
MAC ADDR    VLAN ID      STATE        PORT INDEX          AGING TIME(s)
0023-893a-4cf0    1      learned      GigabitEthernet1/0/1     AGING
0023-893a-4cf0  4043     learned      GigabitEthernet1/0/3     AGING
000f-e207-f2e0    1      learned      GigabitEthernet1/0/1     AGING
3ce5-a683-1fc2    2      learned      GigabitEthernet1/0/3     AGING
             ---  4 mac address(es) found  ---
```

② 车载 AP 主链路切换时，轨旁 AP 上行设备应及时更新组播表项，使用命令检查轨旁 AP 上行设备的组播表项是否及时更新。

```
[S75E]display igmp-snooping group  vlan 300 verbose
  Total 2 IP Group(s).
  Total 2 IP Source(s).
  Total 2 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):300.
    Total 2 IP Group(s).
    Total 2 IP Source(s).
    Total 2 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:239.1.1.1
        (0.0.0.0, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 1 port.
            Eth1/0/2              (D) ( 00:02:31 )
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            Eth1/0/2
```

（8）检查 MLSP-proxy 参数

车载 MR 主链路切换伴随着轨旁 AP 上行设备转发表项的刷新。因此，要求 MESH 主链路切换时 MR 通过代发报文更新轨旁 AP 等设备的转发表项。车载 MR 上配置车载主机的 MAC、VLAN 和 IP 信息，主链路切换后代理发送车载主机的 GARP 报文。如果车载 MR 存在二层组播表项，主链路切换前车载 MR 代发组播离开报文，主链路切换之后代发组播加入报文。

命令：*display current-configuration*

例如：检查当前配置信息，核实绑定车载主机信息是否准确。

```
[MR]display current-configuration
wlan mp-policy 1
 link-hold-rssi 21
 link-hold-time 3000
 link-switch-margin 8
 link-maximum-number 3
 mlsp enable
 mlsp-proxy mac-address 3822-d696-1500 vlan 300 ip 172.17.150.254
```

（9）排除干扰

桥接网络 MESH 链路使用固定信道转发数据，信道拥塞将影响数据转发质量，设备空口利用率是衡量 MESH 链路拥塞率的重要指标，空口利用率高则信道拥塞率高，反之亦然。影响空口利用率常见原因为 WLAN 干扰、非 WLAN 干扰、弱信号、低速率等，如何分析且看下面分解。

① 判断是系统内部干扰还是外部干扰。系统内部干扰即轨旁 AP 之间相互干扰，可以将

临近几个轨旁 AP 同时关闭射频口，查看中间这个 AP 的空口利用率，如果空口利用率降低，则说明干扰源来自系统内，反之则说明干扰源来自于系统外部。

命令：*display ar5drv x channelbusy ST*

例如：查看信道空口利用率。

```
[MR-hidecmd]display ar5drv 2 channelbusy
ChannelBusy information
 Ctl Channel:      11      Channel Band: 20M
 Ext Channel:
 Record Interval(s):    9
 Date/Month/Year: 17/11/2011
        Time(h/m/s):   CtlBusy(%)  TxBusy(%)    RxBusy(%)    ExtBusy(%)
 01       21:57:37         64          1            56            0
 02       21:57:28         64          1            56            0
```

② 如果是系统内部干扰：系统内部干扰来自轨旁 AP 之间信号相互干扰，或者低速率报文占用信道资源，调整轨旁 AP 发射功率以及禁用低速率可以达到优化目的。

命令：*max-power x*

dot11g diabled-rate x

(a) 调整轨旁 AP 射频口发射功率。

```
[MR]interface wlan-radio 2
[MR-interface-WLAN-Radio2]max-power XX
```

(b) 禁用车载 MR 以及轨旁 AP 低速率。

```
[MR]interface wlan-radio 2
[MR-WLAN-RRM]dot11g disabled-rate 1 2 5.5 6 9 11 12
[MR-WLAN-RRM]display this
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 18
 dot11g supported-rate 24 36 48 54
 dot11g disabled-rate 1 2 5.5 6 9 11 12
```

说明：如果轨旁 AP 是 FIT AP，必须在 AC 上禁用低速率。

③ 如果是系统外部干扰：通过空口利用率可以定性分析是 WLAN 干扰或非 WLAN 干扰，如果 CtlBusy 远大于 TxBusy+RxBusy，则可以推断外界干扰为非 WLAN 干扰，建议联系客户排除外界干扰源保证信道质量，如果不能排除外界干扰，建议更换 MESH 信道或者更换桥接工作频段。

命令：*channel xx*

radio-type dot11g

例如：更改车载 MR 桥接协议以及桥接信道。

```
[MR]interface wlan-radio 2
[MR-WLAN-radio2]radio-type dot11g
[MR-WLAN-radio2]channel 11
```

说明：轨旁AP和车载MR桥接协议以及信道必须同时修改，否则无法建立MESH链路。

（10）优化切换信号阈值

主备链路信号切换阈值设置不合理，将影响主备链路平滑切换。分析车载MR异常切换日志，如果异常切换与信号相关，则需优化主链路切换信号阈值。车载MR运动轨迹弯道多或者上下坡居多场景，可以适当降低参数数值。

命令：*link-switch-margin x*

例如：调整主链路信号切换阈值为8，默认值为10。

```
[MR]wlan mp-policy 1
[MR-wlan-mp-policy-1]link-switch-margin  8
```

（11）优化主链路保持时间参数、减少频繁切换

桥接网络MESH链路频繁切换时可能导致丢包，为了避免主链路频繁切换，软件设置主链路必须保持一定时间才能切换。

通过检查主链路切换日志找到异常切换日志，分析主链路异常切换与前一次主链路切换时间，根据时间差值分析主链路保持时间，如果主链路保持时间等于或者接近设定阈值，可适当调高主链路保持时间，主链路保持时间经验数据是3000ms。

命令：*link-hold-time 3000*

例如：调整主链路保持时间为3000ms，如果车载MR运动轨迹弯道或者上下坡居多，可适当调小该参数。

```
[MR]wlan mp-policy 1
[MR-wlan-mp-policy-1]link-hold-time 3000
```

（12）检查轨旁AP

天线主波瓣指向车载MR运动方向，轨旁AP天线方位角根据天线安装高度和车载MR天线高度决定，尽可能保证轨旁AP天线和车载MR天线覆盖交叉区域更大。在上下坡或者弯道区域，可能存在覆盖不足，可以通过增大功率或者使用左右线AP交叉覆盖方式。如果调整功率且左右线交叉覆盖依然不能满足覆盖要求，建议增加AP覆盖。

对于AP信号覆盖满足要求，但MESH链路信号弱，可以从以下几方面排查。

① 优化发射功率。调整射频口的发射功率，增加信号覆盖。

命令：*max-power xx*

例如：调整轨旁AP发射功率为18。

```
[轨旁 AP]interface wlan-radio 2
[轨旁 AP-interface-WLAN-Radio2]max-power 18
```

说明：调整功率时优先考虑信号覆盖，在满足信号覆盖基础上再优化系统内部干扰。

② 检查工程连接。如果动车测试整条线主链路信号均偏弱，需检查车载MR工程连接是否符合规范；如果个别轨旁AP信号偏弱，则需检查轨旁AP工程连接是否符合规范，工程连接是否规范的标准包括。

（a）确认轨旁AP是否正常启动，可以通过Console口登录或者面板指示灯确认。

（b）确认轨旁AP信道设置是否正确。

（c）检查天线馈线是否连接在正确的AP天馈口上（2.4G或5G）。

(d) 检查AP馈线口与天线馈线口连接是否可靠。

(e) 检查AP与天线极化连接方式,对于双流两个馈线口的AP需要分别连接天线水平和垂直极化方向;对于双流三个馈线口的AP,AP馈线口1和3分别连接天线水平和垂直极化方向;对于三流三馈线口的AP,遵循AP馈线口1和3分别连接水平和垂直极化方向,余下馈线口连接天线剩余馈线口。

(f) 检查网口连接处、馈线连接处防水防尘处理是否标准,室外AP还需做好接地、防雷处理。

③ 检查天线安装方向:直道,主波瓣平行轨道方向;弯道,主波瓣稍往轨道内侧覆盖。天线方位角和下倾角共同决定天线主波瓣方向,桥接链路要求两端天线主波瓣方向尽可能重叠,同时天线极化方向需要一致。在MESH链路已经建立但是信号较弱,或者可以收到对端Probe报文但无法建立MESH链路情况下,可以先固定一端天线角度,左右调整另一端天线方位角,或者上下调整下倾角,增加两边天线主波瓣重叠度,达到优化桥接信号的目的,如图7-28所示。



图7-28 调整天线角度

(13) 检查AC配置

轨旁AP为FIT AP,AC集中控制、管理轨旁AP。轨旁AP注册成功后,AC集中控制下发配置,需要确认AC配置是否正确,下发到AP的配置是否成功。

① 开启端口安全。

```
[AC] port-security enable
```

② 配置MESH接口,将MESH接口配置为Trunk模式并放通业务VLAN,车载AP和AC上MESH接口配置的密钥必须相同。

```
[AC]interface WLAN-MESH 1
[AC-wlan-mesh1]port link-type trunk
[AC-wlan-mesh1]port trunk permit vlan X    //X为车地通信的业务vlan-id
[AC-wlan-mesh1]port-security port-mode psk
[AC-wlan-mesh1]port-security tx-key-type 11key
[AC-wlan-mesh1]port-security preshared-key pass-phrase abcd0001
```

③ 配置MESH服务,车载MR和AC上配置的MESH-ID必须一致,否则无法建立MESH链路。

```
[AC]wlan mesh-profile 1
[AC-wlan-mshp-1]mesh-id sys_mesh
[AC-wlan-mshp-1]bind WLAN-MESH 1
[AC-wlan-mshp-1]mesh-profile enable
```

④ 为了避免轨旁有线网络环路，必须配置轨旁 AP 之间禁止建立临时链路，以及不主动建立 MESH 链路。默认情况下，轨旁 AP 之间可以建立临时 MESH 链路；轨旁 AP 注册到 AC 之后，相互使用新配置建立 MESH 链路；当轨旁 AP 之间建立 MESH 后，与有线网络形成环路，将影响业务转发以及和 MR 的 MESH 链路建立。

在 AC 上创建 MP-policy，配置轨旁 AP 之间禁止建立临时链路，以及不主动建立 MESH 链路，并将策略应用到 AP 模板上。

```
[AC]wlan mp-policy rail_policy
[AC-wlan-mp-policy-rail_policy]undo link-initiation enable
[AC-wlan-mp-policy-rail_policy]undo role-authenticator enable
[AC-wlan-mp-policy-rail_policy]undo temporary-link enable
```

⑤ 全局模式下使能 mesh-profile。

```
[H3C]mkd-service enable mesh-profile 1
```

⑥ 配置 map 文件，车载 MR 通过 MESH 链路将数据转发给轨旁 AP，轨旁 MR 对于 MESH 链路的数据通过本地转发模式向上行交换机转发数据。因此，轨旁 AP 上需要创建业务 VLAN、将以太网口配置为 Trunk 并放通业务 VLAN。如果存在组播业务，需要开启二层组播协议且配置未知组播丢弃功能，map 文件下发是否生效可以 Telnet 到 AP 上通过查看当前配置来确认。

```
igmp-snooping                          //如果没有组播业务可以省略
vlan 100
igmp-snooping enable                   //如果没有组播业务可以省略
igmp-snooping drop-unknown             //如果没有组播业务可以省略
interface Ethernet1/0/1
port link-type trunk
port trunk per vlan 1 100
quit
```

说明：*在本地创建 txt 文件，将命令写入 txt 文件，编辑好文件后上传到 AC Flash→CF 卡，即为 map 文件。*

⑦ 创建 AP 模板，在模板视图下调用 map 文件并开启 MESH Portal 服务。MESH 使用固定信道，车载 MR 和轨旁 AP 需要配置相同信道，在射频口下指定 MESH 链路信道，并调用 MP 策略和 mesh 服务。

```
[H3C]wlan ap testap1 model WA2210X-GE
[H3C-wlan-ap-testap1]map-configuration map.txt
[H3C-wlan-ap-testap1]serial-id 210235A36L0089000035
[H3C-wlan-ap-testap1]portal-service enable
[H3C-wlan-ap-testap1]radio 1
[H3C-wlan-ap-testap1-1]channel 13
[H3C-wlan-ap-testap1-1]mp-policy rail_policy
[H3C-wlan-ap-testap1-1]mesh-profile 1
[H3C-wlan-ap-testap1-1]radio enable
```

(14) 检查 MR 配置

① 开启端口安全。

```
[MR] port-security enable
```

② 配置 MESH 接口，将 MESH 接口配置为 Trunk 模式并放通业务 VLAN，车载 AP 和 AC 上 MESH 接口配置的密钥必须相同。

```
[MR]interface WLAN-MESH 1
[MR-wlan-mesh1]port link-type trunk
[MR-wlan-mesh1]port trunk permit vlan X    //X 为车地通信的业务 vlan-id
[MR-wlan-mesh1]port-security port-mode psk
[MR-wlan-mesh1]port-security tx-key-type 11key
[MR-wlan-mesh1]port-security preshared-key pass-phrase abcd0001
```

③ 配置 MESH 服务，车载 MR 和 AC 上配置的 MESH-ID 必须一致，否则无法建立 MESH 链路。

```
[MR]wlan mesh-profile 1
[MR-wlan-mshp-1]mesh-id sys_mesh
[MR-wlan-mshp-1]bind WLAN-MESH 1
[MR-wlan-mshp-1]mesh-profile enable
```

④ MESH 链路需要协议报文控制链路稳定性，大量的控制报文将占用 MESH 链路带宽，为了减少控制报文占用 MESH 带宽，MESH 技术使用信号阈值与链路条数减少控制报文；同时，为了保证 MESH 链路稳定切换，需要配置主链路保持时间和主备链路切换信号阈值；主链路切换之后，需要及时更新轨旁设备的 MAC 地址表项，在 MR 上需要定义车载主机信息，MESH 链路切换之后，车载 MR 代理发送 GARP 更新轨旁设备表项。

```
[AC]wlan mp-policy rail_policy
[AC-wlan-mp-policy-rail_policy]link-switch-margin 8
[AC-wlan-mp-policy-rail_policy]link-hold-rssi   21
[AC-wlan-mp-policy-rail_policy]link-maximum-number 3
[AC-wlan-mp-policy-rail_policy]link-hold-time 3000
[AC-wlan-mp-policy-rail_policy]mlsp enable
[AC-wlan-mp-policy-rail_policy]mlsp-proxy mac-address 000d-56dc-ba64 vlan 100 ip 10.2.4.9
```

⑤ MR 全局创建业务 VLAN，并配置以太网口放通业务 VLAN。如果存在组播业务，需要在全局视图和 VLAN 视图开启二层组播协议，并开启未知组播丢弃。

```
[MR]igmp-snooping                                  //如果没有组播业务可以省略
[MR]vlan 100
[MR--igmp-snooping]igmp-snooping enable            //如果没有组播业务可以省略
[MR--igmp-snooping]igmp-snooping drop-unknown      //如果没有组播业务可以省略
[MR]interface Ethernet1/0/1
[MR-GigabitEthernet1/0/1] port access vlan 100
```

⑥ 调用 MP 策略和 MESH 服务，并配置固定信道，信道号和轨旁 AP 保持一致。

```
[MR]interface WLAN-Radio1/0/2
[MR-wlan-Radio1/0/2]channel 13
[MR-wlan-Radio1/0/2]mp-policy 1
[MR-wlan-Radio1/0/2]mesh-profile 1
```



无线终端硬件故障排查
吴骋骐
表示上一步结果正常
表示上一步结果出现问题
开始
指示灯是否正常
是否正常启动
环境及硬件状态是否正常
端口自检、光口自检
是否正常上电
检查启动打印信息里异常记录
拨打热线
400-810-0504
寻求帮助

1. 开始

无线终端硬件故障排查，首先观察外观指示灯是否正常，其次排查供电是否正常，然后登录查看是否正常启动，最后通过命令行排查端口及设备状态。

2. 流程图相关操作说明

(1) 指示灯是否正常

指示灯状态可以协助判断当前 AP 工作状态，观察 AP 面板呼吸灯和接口指示灯状态，AP 面板呼吸灯和接口指示灯状态说明请参考各型号 AP 的安装指导手册。

(2) 是否正常上电

检查 POE 受电是否正常，POE 供电端口及网线是否正常。

一般情况下，根据 AP 本身功耗选择合标的 POE 端口即可，如出现 POE 无法受电，在相同 POE 供电端口及网线的条件下，对相同型号的 AP(功耗相当的 AP)进行替换测试即可确认故障。

本地电源供电环境可以替换电源适配器测试。

(3) 是否正常启动

开机或运行过程重启，常见为下面两种情况。

① 找不到启动文件，确认启动文件本身是否正常或 Flash 故障导致启动文件异常，此时可以使用 Ctrl+F 组合键格式化 Flash 后重新加载启动文件。需确认 AP 工作模式和软件版本是否一致，如格式化过程报错，需要更换 AP。

② BootWare 提示 CRC 错误：使用 Ctrl+T 组合键在设备开始启动时测试，如出现内存 Fail 则内存故障，需要更换 AP。

(4) 检查启动打印信息里异常记录

设备上电后，Console 接口打印启动信息是否存在异常。在确认 AP 启动异常后，在许可的操作范围内，先尝试进行“三板斧”(重启，格式化，重新导版本)操作，如果故障依旧可参照本文举例问题处理，若再不行请收集相关信息拨打 400 热线。

① 如果 Local log 中见到如下报错信息，可以确认硬件故障。

(a) Exception Name：Bus error exception (data load or store)!

(b) Check net params crc error，use the default value!

(c) Exception nesting occurred on vcpu 0!

Fatal Error，Suspend System now!

② 如果出现以下信息，一般为版本不配套或异常导致，建议 Bootrom 下格式化 Flash 后重新上传正确软件版本的。

(a) Unknow equipment tag：WA2610-AGN，cannot initialize extra attribute!

(b) !ulBoardType ERROR!!!

③ 如果出现以下信息，多为射频卡异常或丢失，需要返修。

(a) Device attach error! 同时伴随反复重启。

(b) display current-configuration 看到的 interface WLAN-Radio 接口数与设备型号不符。

(c) Exception

Exception Number: 0x10

Exception Name: DATA EXCEPTION

Exception Instruction: 0x003BD2A4

Exception Slot: 0

Exception Task: N/A (TID: 0xffffffff)

Exception Stack Base: 0xffffffff

(d) Calling reschedule functions in IRQ context is not allowed!

Fatal Error, Suspend System now!

④ 如果出现以下信息，多为 Bootrom 异常导致，可使用 FAT AP 版本内的. btw 文件升级基本段

(a) Boot ROM program does not exist.

(b) Reserved Instruction Exceptionion

Exception Program Counter: 0x81200000

Status Register: 0x1000c000

Cause Register: 0x30800028

Task: 0x817f61e0 "tBoot"

(c) AP 启动过程中没有 Press Ctrl+B to enter extended boot menu...但是仍然可以进入系统命令行。

(d) System is starting...

readed value is 9170ce2a , expected value is 55555555

DRAM test fails at: 803c0004

DRAM test fails at: 803c0004

Fatal error! Please reboot the board.

(5) 环境及硬件状态是否正常

① 环境状况。

命令：*display environment*

例如：各传感器温度应处于低温告警门限与一般级高温告警门限之间，如出现异常温度告警，比如－1℃、255℃等，一般是软件版本问题或温度传感器硬件故障，需要更换 AP。

```
<H3C>display environment
 System Temperature information (degree centigrade):
----------------------------------------------------
 SlotNo      Temperature        Lower limit       Upper limit
 1           255                 5                  60
```

② AP 硬件运行状况。

命令：*display device*

例如：正常应该是 Normal，出现 Fault 一般为故障。

```
<H3C>display device
 Slot No.   Board Type              Status     Max Ports
 1          WA2620i-AGN Board       Fault       4
```

(6) 端口自检、光口自检

① 检查以太网口是否正常,检查上联设备端口及网线是否正常。

除了端口自检的几种常见故障外,有的时候会出现以太网口无法 Up 的情况,此时处理方法可参考 POE 故障检测,在相同 POE 供电端口及网线的条件下,对相同型号的 AP(功耗相当的 AP)进行替换测试即可确认故障。

命令:*display interface brief*

例如:如果显示 GE1/0/1 端口状态为 half,需要确认是否两端配置不一致导致。

```
<H3C>display interface brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                Up   Up(s)    --
Vlan1                Up   Up       3.1.1.1
WLAN-Radio1/0/1      Up   Up       --
WLAN-Radio1/0/2      Up   Up       --

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed   Duplex Type PVID Description
GE1/0/1              Up   1G(a)   H(a)   T    1
```

② 是否没有必要启动流控端口配置流控。

命令:*display current-configuration interface*

例如:查看 GE1/0/1 配置,开启了 Flow Control 配置。一般建议关闭该端口流控:Undo Flow Control。

```
<H3C>display current-configuration interface
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 flow-control
```

③ 是否有比较频繁的端口 Up/Down。

命令:*display logbuffer*

例如:查看 GE1/0/1 频繁 Up/Down ,需要检查线路和中间连接的光电转换器,千兆端口检查光功率是否处于临界值,检查两端配置是否一致。

```
<H3C>display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 15
```

```
%Dec 30 23:25:27:468 2011 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Up.
%Dec 30 23:25:27:468 2011 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Down.
%Dec 30 23:25:27:469 2011 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Up.
%Dec 30 23:25:27:469 2011 H3C IFNET/3/LINK_UPDOWN: GigabitEthernet1/0/1 link status is Down.
```

④ 端口出/入方向是否有大量的错误报文。

命令：*display interface GigabitEthernet*

例如：查看 GE1/0/1 入方向出现大量 CRC 错包，需检查线路质量，中间连接的光电转换器；两端配置是否一致？是否一端为强制而对端为协商？H3C 设备与其他厂商设备互连，建议光口速率和双工设置要完全一致。光口是否有 CRC 错误？是否在增长？检查光功率是否处于临界值？可以通过更换光模块、更换尾纤或清洗光模块连接器的方式解决。

```
<H3C>display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: Up
Last clearing of counters: Never
 Last 300 seconds input: 0 packets/sec 14 bytes/sec 0%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
 Input (total): 602789 packets, 147083765 bytes
         126789 unicasts, 0 broadcasts, 590 multicasts, - pauses
 Input (normal): 602 packets, 147083 bytes
         12 unicasts, 0 broadcasts, 590 multicasts, - pauses
 Input: 6734 input errors, 0 runts, 0 giants, - throttles
3214 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, - parity errors
 Output (total): 12 packets, 816 bytes
         10 unicasts, 2 broadcasts, 0 multicasts, - pauses
 Output (normal): 12 packets, 816 bytes
         10 unicasts, 2 broadcasts, 0 multicasts, - pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, 0 no carrier
```


李晨光
开始
表示上一步结果正常
表示上一步结果出现问题
无线终端丢包问题定位故障排查
终端能否ping通网关
判断有线网络是否正常
判断终端在线状态是否正常
排查无线接入问题
请排查有线网络丢包
根据终端状态依次改善网络状况
判断无线空口利用率是否正常
判断无线空口统计是否正常
通过软件优化、硬件调整降低空口繁忙度
排查DHCP问题
排除空口干扰降低底噪干扰
拨打热线400-810-0504寻求帮助
收集终端抓包、空口抓包、debugging信息

1. 开始

WLAN 在使用过程中，有时候会发现无线终端（STA）在 ping 其他设备时，会出现连续丢包现象。这种情况下可能还伴随 ping 延时增大（几百毫秒），并导致一些应用感觉不是很好，例如下载速度变慢、视频出现抖动等。这种情况是 WLAN 网络中比较棘手的问题，一方面 WLAN 本身有一个复杂的、不容易评估的空间媒质，导致空口的不稳定性；另一方面还要综合考虑整个有线、无线网络的网络配置和性能。

如图 7-29 所示是一个典型的 WLAN 基本网络构成（FIT AP 组网方式），当 Station ping 服务器丢包严重时，需要按照报文转发途径来考虑丢包的可能性。

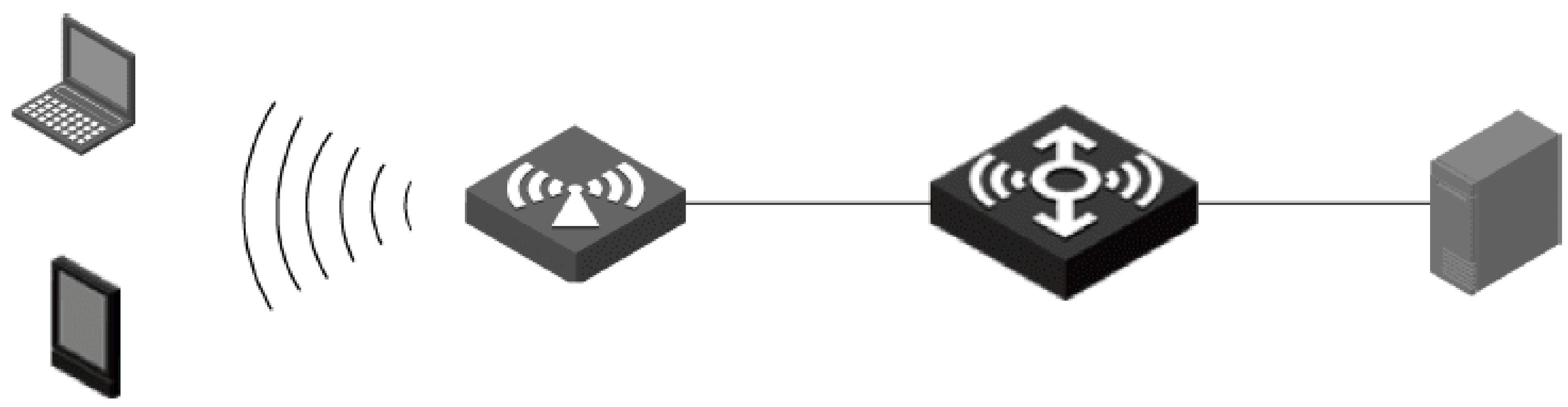


图 7-29 典型的 WLAN 基本网络构成

定位故障的思路如下。

首先，通过测试判断终端能否正常连接、获取地址。

其次，判断有线网络是否存在丢包问题。

再次，判断无线终端状态、空口利用率、空口质量、底噪是否正常。

最后，通过收集 debugging 信息分析问题原因。

2. 流程图相关操作说明

(1) 终端能否 ping 通网关

① ping 测试具体操作。

命令：*ping 192.168.1.3*

例如：通过命令查看，可以确认当前网络丢包属于哪种类型。

```
D:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=19ms TTL=255
Reply from 192.168.1.3: bytes=32 time=4ms TTL=255
Reply from 192.168.1.3: bytes=32 time=3ms TTL=255
Reply from 192.168.1.3: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 19ms, Average = 7ms
```

② 无线网络丢包说明。

从目前的协议分析和实际应用来看，无线网络可能无法实现真正的零丢包。空口利用率

正常、无干扰的情况下,3%以内的丢包是可以接受的范围。

(2) 判断有线网络是否正常

① 如果网关不在 AC 上,需要做终端 ping AC 地址的测试。

第一,如果 ping 网关异常但是 ping AC 正常,则需要排查 AC 至网关二层网络。

第二,如果 ping 网关、AC 均异常,则需要排查有线丢包。

② 如果终端在线则直接通过命令行查到当前 AP 地址,然后通过 AC ping AP 判断 AC 到 AP 的有线网络链路状态,如果终端不在线,则直接进入下一个环节。

第一,查找当前终端所连接 AP 的名称。

命令: *display wlan client mac-address 0024-d79c-af4c verbose*

例如: 通过命令查看,可以确认终端当前连接 AP 的名字。

```
[AC]display wlan client mac-address 0024-d79c-af4c verbose
…
AP Name                          : ap1
```

第二,查看终端当前连接 AP 的地址。

命令: *display wlan ap name* ***ap1*** *verbose*

例如: 通过命令查看,可以确认 AP1 的地址为 192.168.1.6,在线时长为 22 个小时,如果在线时间很短,则证明 AP 注册存在问题,需要参考注册指导排查问题原因。

```
[AC]display wlan ap name ap1 verbose
 …
 Up Time(hh:mm:ss)                : 22:06:21
 …
 IP Address                       : 192.168.1.6
```

第三,在 AC 上 ping AP 地址,观察网络质量。

命令: *ping 192.168.1.6*

例如: 通过命令查看,可以确认 AC 到 AP 这段有线网络是否正常。

```
[AC]ping 192.168.1.6
  PING 192.168.1.6: 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.6: bytes=56 Sequence=1 ttl=255 time=1 ms
…
  --- 192.168.1.6 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

(3) 请排查有线网络丢包

通过逐级 ping、抓包方式明确具体丢包的位置,再检查二层、三层设置是否符合规范,涉及具体协议可参考各协议的故障排查指导。

(4) 排查无线接入问题

① 可以在 AC 上通过命令查看用户的关联状态。

命令: *display wlan client mac-address 0024-d79c-af4c*

例如: 通过命令查看无线用户有无关联 AC。

```
[AC]display wlan client mac-address 0024-d79c-af4c
 Total Number of Clients               : 1
                              Client Information
------------------------------------------------------------------------------
MAC Address      User Name   APID/RID      IP Address      VLAN
------------------------------------------------------------------------------
0024-d79c-af4c       -NA-          1    /1        192.168.1.8          1
```

② 排查无线接入问题。

第一,检查终端无线网卡是否正常打开。

第二,检查是否在终端服务中开启无线服务,例如 Windows 操作系统中,要开启 Wireless Zero Configuration。

在"服务"中找到 Wireless Zero Configuration,并开启该服务即可,如图 7-30 所示。

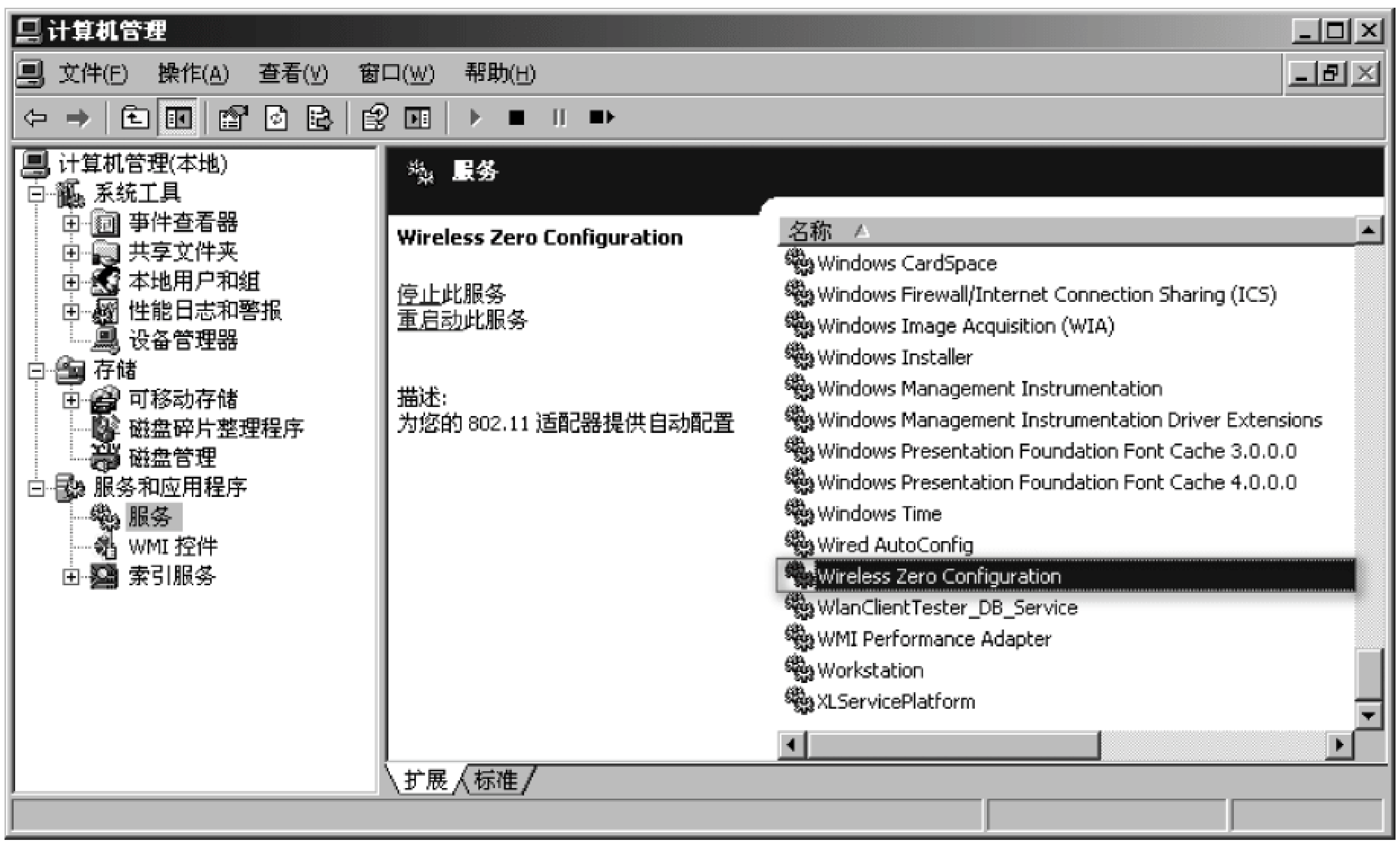


图 7-30 开启 Wireless Zero Configuration

第三,检查终端是否工作在正常的无线终端模式,如果错误的设置成 AP 模式则无法作为无线终端使用。

第四,检查终端是否关联正确的 SSID。

(5) 排查 DHCP 问题

① 在 STA 上单击"开始"按钮→"运行"→输入"cmd"→按回车键,通过命令行查看终端地址获取情况。

命令:*ipconfig /all*

例如:通过命令查看,可以确认本机获取 IP 地址 192.168.1.8。

```
D:\>ipconfig /all
Ethernet adapter 无线网络连接:

Ethernet adapter 无线网络连接:
...
IP Address. . . . . . . . . . . . : 192.168.1.8
```

② 如果没有正常获取地址，则需要排查 DHCP 问题。

请参考：IP 业务——DHCP 排查模块。

（6）判断终端在线状态是否正常

命令：*display wlan client mac-address 0024-d79c-af4c verbose*

例如：通过命令查看，可以确认 MAC 为 0024-d79c-af4c 的终端正常上线。

```
[AC]display wlan client mac-address 0024-d79c-af4c verbose
 Total Number of Clients              : 1
                              Client Information
-----------------------------------------------------------------
 MAC Address                          : 0024-d79c-af4c
 ...
 Power Save Mode                      : Active
 ...
 RSSI                                 : 33
 Rx/Tx Rate                           : 300/300
 ...
 Up Time (hh:mm:ss)                   : 00:01:05
```

① Power Save Mode 表示终端状态，当终端处于休眠状态则 ping 延时会比较大，一般会大于 Beacon 间隔。

② RSSI 表示 AP 收到的终端信号强度，信号强度应该尽量达到 30 之上。

③ Rx/Tx Rate，如果 Rx Rate 始终保持在较低速率（例如 1、2、11），该客户端所在的环境可能丢包比较严重，需要对空间使用情况进行分析。

④ Up Time 表示用户在线时间，如果 Up Time 时间比较短，而该用户已经长时间使用无线网络，需要考虑该用户是否出现过漫游。

（7）根据终端状态依次改善网路状况

① 无线用户的信号强度 RSSI 偏低（低于 25），则需要分析一下该用户状态以及对整个网络的影响，尽量提高无线用户的信号。可以通过调整天线、增加 AP 的方式改善信号覆盖。

② 无线用户的 Rx 和 Tx 速率偏低：通常说明空口环境不是特别好、甚至丢包比较多，需要进行空口的分析（例如信道占用情况、确认网络流量），适当进行流量控制或者无线用户的限速。

③ 无线用户漫游比较频繁（在各个 AP 上持续的时间都比较短）：可以适当的调整这台客户端连接的 AP 的发射功率减少用户的漫游，或者将网卡的漫游主动性调低。

④ 终端处于休眠状态则 ping 延时会比较大，一般会大于 Beacon 间隔。

（8）判断无线空口利用率是否正常

① 需要登录 AP 查看空口利用率。

第一，查找当前终端所连接 AP 的名称。

命令：*display wlan client mac-address 0024-d79c-af4c verbose*

例如：通过命令查看，可以确认当前终端所连接 AP 的名字。

```
[AC]display wlan client mac-address 0024-d79c-af4c verbose
...
AP Name                                 : ap1
...
```

第二，查看当前终端所连接的 AP 的地址。

命令：*display wlan ap name* **ap1** *verbose*

例如：通过命令查看，可以确认 AP1 的地址为 192.168.1.6

```
[AC]display wlan ap name ap1 verbose
…
IP Address                    : 192.168.1.6
…
```

第三，打开 AP 远程登录开关，通过 AC 登录到 AP 上。

命令：*[AC]_h*

[AC-hidecmd]wlan ap-execute **ap2** *telnet enable*

[AC-hidecmd]wlan ap-execute **ap2** *exec-control enable*

[AC-hidecmd]quit

[AC]quit

<AC>telnet **192.168.1.6**

例如：通过在 AC 上 Telnet，可以成功登录到终端所关联的 AP 上。

```
[AC]_h
Now you enter a hidden command view for developer's testing, some commands may affect operation by
wrong use, please carefully use it with our engineer's direction.
[AC-hidecmd]wlan ap-execute ap2 telnet  enable
[AC-hidecmd]wlan ap-execute ap2 exec-control enable
[AC-hidecmd]quit
[AC]quit
<AC>telnet 192.168.1.6
```

第四，查看信道利用率，判断空口繁忙情况。

命令：*display ar5drv 1/2*（单频 AP 只有一个射频口，双频 AP 则 1 表示 5G 视频口，2 表示 2.4G 射频口）*channelbusy*

例如：通过命令查看，AP 的 5G 射频口空口目前处于正常状态，当 CtlBusy 高于 60 时，则表示空口繁忙。

```
<AP>sys
System View: return to User View with Ctrl+Z.
[AP]_h
[AP-hidecmd]display ar5drv 1 channelbusy
ChannelBusy information
 Ctl Channel:      149      Channel Band: 40M
 Ext Channel:               Above
 Record Interval(s):   9
 Date/Month/Year: 03/05/2013
        Time(h/m/s):    CtlBusy(%) TxBusy(%)   RxBusy(%)   ExtBusy(%)
 01      11:18:35          68         37          28          0
 02      11:18:26          67         36          29          0
 03      11:18:17          63         35          26          0
 04      11:18:08          78         40          33          0
 05      11:17:59          81         43          36          0
…
```

② 如果一个 AP 用户大于 15，且用户使用频繁，则空口利用率必然会比较高。

命令：*display wlan client ap* ***ap2***

例如：通过命令查看，可以确认当前终端所关联的 AP 下总共有 15 个终端。

```
[AC]display wlan client ap ap2
 Total Number of Clients                : 15
                                        Client Information
--------------------------------------------------------------------------------
MAC Address      User Name          APID/RID IP Address             VLAN
--------------------------------------------------------------------------------
0024-d79c-af4c    -NA-              2    /1    192.168.1.8             1
...
```

(9) 通过软件优化、硬件调整降低空口繁忙度

请参考：无线产品维护手册——空口优化维护手册。

(10) 判断无线空口统计是否正常

① 需要登录 AP 查看统计信息是否正常。

第一，查找当前终端所连接 AP 的名称

命令：*display wlan client mac-address 0024-d79c-af4c verbose*

例如：通过命令查看，可以确认当前终端所连接 AP 的名字。

```
[AC]display wlan client mac-address 0024-d79c-af4c verbose
...
AP Name                                : ap1
...
```

第二，查看当前终端所连接的 AP 的地址。

命令：*display wlan ap name* ***ap1*** *verbose*

例如：通过命令查看，可以确认 AP1 的地址为 192.168.1.6

```
[AC]display wlan ap name ap1 verbose
...
IP Address                        : 192.168.1.6
...
```

第三，打开 AP 远程登录开关，通过 AC 登录到 AP 上。

命令：*[AC]_h*

[AC-hidecmd]wlan ap-execute ***ap2*** *telnet enable*

[AC-hidecmd]wlan ap-execute ***ap2*** *exec-control enable*

[AC-hidecmd]quit

[AC]quit

<AC>telnet ***192.168.1.6***

例如：通过在 AC 上 telnet，可以成功登录到终端所关联的 AP 上。

```
[AC]_h
Now you enter a hidden command view for developer's testing, some commands may affect operation by
wrong use, please carefully use it with our engineer's direction.
[AC-hidecmd]wlan ap-execute ap2 telnet enable
```

```
[AC-hidecmd]wlan ap-execute ap2 exec-control enable
[AC-hidecmd]quit
[AC]quit
<AC>telnet 192.168.1.6
```

② 查看 AP 空口统计情况，判断空口质量。

命令：*display ar5drv 1/2*（单频 AP 只有一个射频口，双频 AP 则 1 表示 5G 视频口，2 表示 2.4G 射频口）*statistics*

```
[AP-hidecmd]display ar5drv 1 statistics
Radio statistics:
 TxFrameAllCnt          : 40693
 TxFrameAllBytes        : 7293360
Queue statistics
 Queue Number :0          1          2       3        EmergencyQ CAB
 ---------------------------------------------------------------------------
 TxFrameCnt       :152        5745       0       0         1883        2729
 TxUcastFrameCnt:152         3780       0       0         1883        0
 ...
 TxDiscardFrame:2            4          0       0          31          2
 ...
 RadioResetOnErr        : 0
 ...
 BeaconBusyCnt          : 2
 BeaconErrCnt           : 0
 ...
```

说明：

第一，每个 Radio 有 4 个普通发送队列和 1 个紧急发送队列，通常数据报文都走 1 号队列。通常我们主要关注 1 号队列。

第二，TxDiscardFrame 表示此队列丢弃的报文总数，包括发送失败和队列溢出的报文。

第三，TxDiscardFrame/TxUcastFrameCnt 表示丢包率，如果超过 3%的时候就应当警惕了。

第四，RadioResetOnErr 意味着 Radio 芯片复位，会导致丢包，正常情况下不应当出现这个错误。

第五，BeaconBusyCnt 和 BeaconErrCnt 表示 AP 发送 Beacon 的繁忙度及错误统计，此处可以看出空口的质量，如果出现增长则会出现丢包现象。

③ 查看 AP 各个栈的使用情况。

命令：*display ar5drv 1 queue all*

```
[AP-hidecmd]display ar5drv 1 queue all
Name Queue       Head        Tail        DescCount   FrameCount FrameLimit
Rev  0x87806a30  0xa72d3e60  0xa72d3ce0  512         100        512
AC0  0x87806a78  0xa742b540  0xa742b540  0           0          10
AC1  0x87806ab8  0xa742d340  0xa742d340  0           0          10
AC2  0x87806af8  0x00000000  0x00000000  0           0          10
AC3  0x87806b38  0x00000000  0x00000000  0           0          10
Emg  0x878090e8  0xa7429440  0xa7429440  0           0          0
CAB  0x87809068  0xa73e3cc0  0xa73e3cc0  0           0          100
Bcn  0x878090a8  0xa72fd440  0xa72fd440  125959      1          0
Ept  0x878069e8  0xa742c5c0  0xa742c440  4964        0          5000
```

说明：

第一，FrameCount 如果不为零则表示当前报文有积压情况。偶尔的几个报文积压不会引起什么问题，但长时间积压上百个报文就应当引起警惕。通常我们主要关注 AC1（即 1 号队列）。

第二，FrameLimit 表示每个栈的上限。

(11) 排除空口干扰降低底噪干扰

① AP 上查看底噪是否正常。

第一，查找当前终端所连接 AP 的名称。

命令：*display wlan client mac-address 0024-d79c-af4c verbose*

例如：通过命令查看，可以确认当前终端所连接 AP 的名字。

```
[AC]display wlan client mac-address 0024-d79c-af4c verbose
...
AP Name                                : ap1
...
```

第二，查看当前终端所连接的 AP 的地址。

命令：*display wlan ap name* ***ap1*** *verbose*

例如：通过命令查看，可以确认 AP1 的地址为 192.168.1.6。

```
[AC]display wlan ap name ap1 verbose
...
IP Address                       : 192.168.1.6
...
```

第三，打开 AP 远程登录开关，通过 AC 登录到 AP 上。

命令：[AC]_*h*

[AC-*hidecmd*]*wlan ap-execute* ***ap2*** *telnet enable*

[AC-*hidecmd*]*wlan ap-execute* ***ap2*** *exec-control enable*

[AC-*hidecmd*]*quit*

[AC]*quit*

<AC>*telnet* ***192.168.1.6***

例如：通过在 AC 上 telnet，可以成功登录到终端所关联的 AP 上。

```
[AC]_h
Now you enter a hidden command view for developer's testing, some commands may affect operation by
wrong use, please carefully use it with our engineer's direction.
[AC-hidecmd]wlan ap-execute ap2 telnet enable
[AC-hidecmd]wlan ap-execute ap2 exec-control enable
[AC-hidecmd]quit
[AC]quit
<AC>telnet 192.168.1.6
```

第四，查看 AP 空口统计情况，判断空口质量。

命令：*display ar5drv 1/2*（单频 AP 只有一个射频口，双频 AP 则 1 表示 5G 视频口，2 表示 2.4G 射频口）*calibration*（列出合格标准）

例如：当 Value 值高于−80 的时候就需要警惕，可借助仪器分析原因。

```
[AP-hidecmd]display ar5drv 1 calibration
Calibration Information:
  Calibration Enable:    YES
  Calibration Interval:   1000         Reset Radio Count:   0
  iqCalState:            CAL_DONE    I:   62/60/58, Q:   -4/0/-2
  iqCalValid:            True
  NoiseFloor:             -93
  RfGainState:           Inactive
  NF Record:
  Num:     NF Value             time                 AGC-CONTROL
   0          -93          17:54:43:038 10/05/2013   FFFFFFFF
   1          -93          17:54:44:038 10/05/2013   FFFFFFFF
   2          -93          17:54:45:038 10/05/2013   FFFFFFFF
...
```

② 借助分析工具分析。可以使用黄马甲，IEEE 802.11b/g 版本及以上的黄马夹是支持用户检查和确定 AP(接入点)、和 RSSI 信号电平、全频谱扫描等内容。或者使用频谱仪频谱(Spectrum)模式可以对测试点进行频谱与干扰分析。

(12) 收集终端抓包、空口抓包、debugging 信息

定位问题如果终端可以抓包则不需要空口抓包即可，如果是说明、证明问题，则需要进行空口抓包，如果终端不支持抓包，则需要进行空口抓包。

① 终端抓包推荐使用 Wireshark/Ethereal 进行抓包。

第一，为了便于抓包分析，可以在无线客户端 ping 固定大小的报文，例如 130B。

第二，提供抓包信息的时候，收集抓包信息后一定要提供无线客户端的 MAC 地址和 IP 地址。

第三，报文分析时可以根据报文大小，确定是否每一个 ping request 报文都很快有 ping reply 回应消息。

第四，如果两边抓包，可以通过 ping 报文的序列号进行匹配分析，确定两个抓包的相对时间进行对比分析，确定延时情况和报文丢失情况。

第五，在无线笔记本上使用 Ethereal 进行抓包，使用该工具选用无线网卡后，需要将如图 7-31 所示，取消选中“Capture packets in promiscuous mode”复选框，才可以抓包。

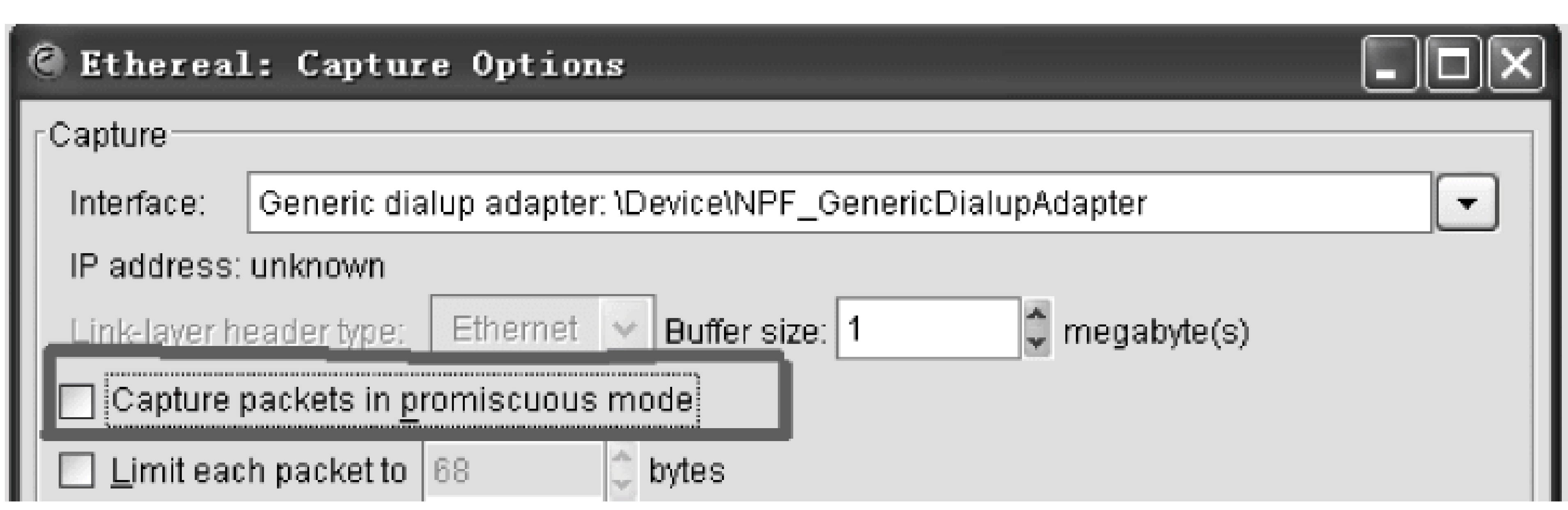


图 7-31　使用 Ethereal 进行抓包设置

② 空口抓包可以使用 Omnipeek/Airmagnet 进行。

首先，在解决问题的时候往往“单兵作战”，很难进行全面的同时抓包分析，但是走到了这一步“已经初步认为空口存在丢包的情况”，也必须想办法进行空口抓包，下面为抓包相关的注意事项。

第一，抓包工具不一定能够将所有的空口报文都抓上来，也就是在分析过程中要充分考虑到可能偶尔有报文接收不上来的情况。

第二，无论使用哪一种抓包，一定要选择当前 Station 所在的信道进行抓包。

第三，ping 有两个方向，一个为 ping request 从 Station 到 AP，另外一个为 ping reply 从 AP 到 Station。

第四，为了报文方便分析，可以 ping 指定大小的报文，例如 130B；特别对于加密的接入一定要采用 ping 特殊长度的报文。

其次，关于抓包分析的分析方法（Omnipeek 的抓包）如图 7-32 所示。

227	IP-123.1.0.99	IP-123.1.1.10	Atheros Comm:0C...		50%	117.0	98	2.228638	PING Req
228	*Atheros Comm:0...*	00:24:01:30:69:04		#	80%	24.0	14	2.228681	802.11 Ack
229	IP-123.1.1.10	IP-123.1.0.99	Atheros Comm:0C...		74%	2.0	98	2.229830	PING Reply
230	00:17:9A:00:7B:47	Ethernet Broad...	Ethernet Broadcast	*	71%	1.0	46	2.260937	802.11 Probe Req
231	Atheros Comm:0...	00:17:9A:00:7B:47	Atheros Comm:0C...	*	81%	1.0	251	2.263292	802.11 Probe Rsp
232	*00:17:9A:00:7B:47*	Atheros Comm:0...		#	72%	1.0	14	2.181822	802.11 Ack
233	[illegible]	Ethernet Broad...	Ethernet Broadcast	*	75%	1.0	78	[illegible]	[illegible]

图 7-32　抓包分析的分析方法

说明：802.11 为了尽量保证单播数据的可靠传输，每一个单播报文都会等待 ACK 确认。例如无线客户端发送一个报文(227)，AP 接收到之后会回应一个 ACK 报文(228)。

相关分析如下。

第一，如果收不到 ACK 确认（Station 没有发送 ACK，或者 AP 没有收到 Station 发送的 ACK），则会进行报文重传。

第二，从 AP 到 Station 以及从 Station 到 AP 都遵循这个规律。

第三，AP 设备默认重传次数为 5 次，Station 重传次数不定。

第四，如果抓包中连续出现多个相同的重传报文，而没有 ACK 报文，说明该报文可能丢失。

第五，根据报文 MAC 地址，可以确定是 AP 到 Station 丢失还是 Station 到 AP 丢失。

最后，下面的判断方法，在一定程度上可以验证是否与网卡关系密切，当前应用过程中还是发现了好多网卡也存在这样或者那样的问题，特别是 11n 网卡。

第一，通常我们习惯上用 Station 去 ping 网关，而很多时候网关不在 AC 上，也就是相当于 AC 连接的一台 PC。更换 Station，再 ping 相同的 PC，看是否还丢包严重。

第二，如果不是，则说明原来 Station 自身很可能存在问题，禁用或者插拔网卡后再重新使用，看能否恢复正常。如果仍然丢包严重，寻求其他帮助。

第三，更换 PC，再用相同的 Station ping，看是否还丢包严重。

第四，如果不是，则说明原来 PC 自身很可能存在问题，寻求其他帮助。实际网络中，通常更换的 PC 可以用 AC 或者中间的交换机替代。

③ 登录 AP 开启 debugging 信息。

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

命令：*<AP>sys*

[AP]_h

[AP-hidecmd] debugging ar5drv 1 phy packet all verbose

[AP-hidecmd]quit

[AP]quit

<AP>terminal monitor

<AP>terminal debugging

④ 通过将抓包信息与 debugging 信息对比，可以判断丢包的具体位置。


表示上一步结果正常
表示上一步结果出现问题
李晨光
开始
无线终端关联失败故障排查
当前SSID是否采用明文方式
判断网络信号强度是否达标
AP关联用户数是否达到上限
检查AP覆盖状态
通过软件调整优化当前网络关联用户数
增强问题区域信号覆盖
是否存在备份AC
通过硬件调整增加当前网络容量
检查WIDS黑白名单配置
检查主备AC的配置并修改一致
新建明文SSID,测试终端能否关联成功
收集log、trap及debugging信息
拨打热线 400-810-0504寻求帮助

1. 开始

无线客户端接入 802.11 无线网络的过程分为以下 4 个步骤，如图 7-33 所示。

① STA 通过主动扫描或者被动侦听搜索附近存在的 AP。

② STA 选择 AP 后，向其发起 Authentication 过程。

③ 通过 Authentication 后，STA 发起 Association 过程。

④ 通过 Association 后，STA 和 AP 之间链路已建立，可以互相收发数据报文。

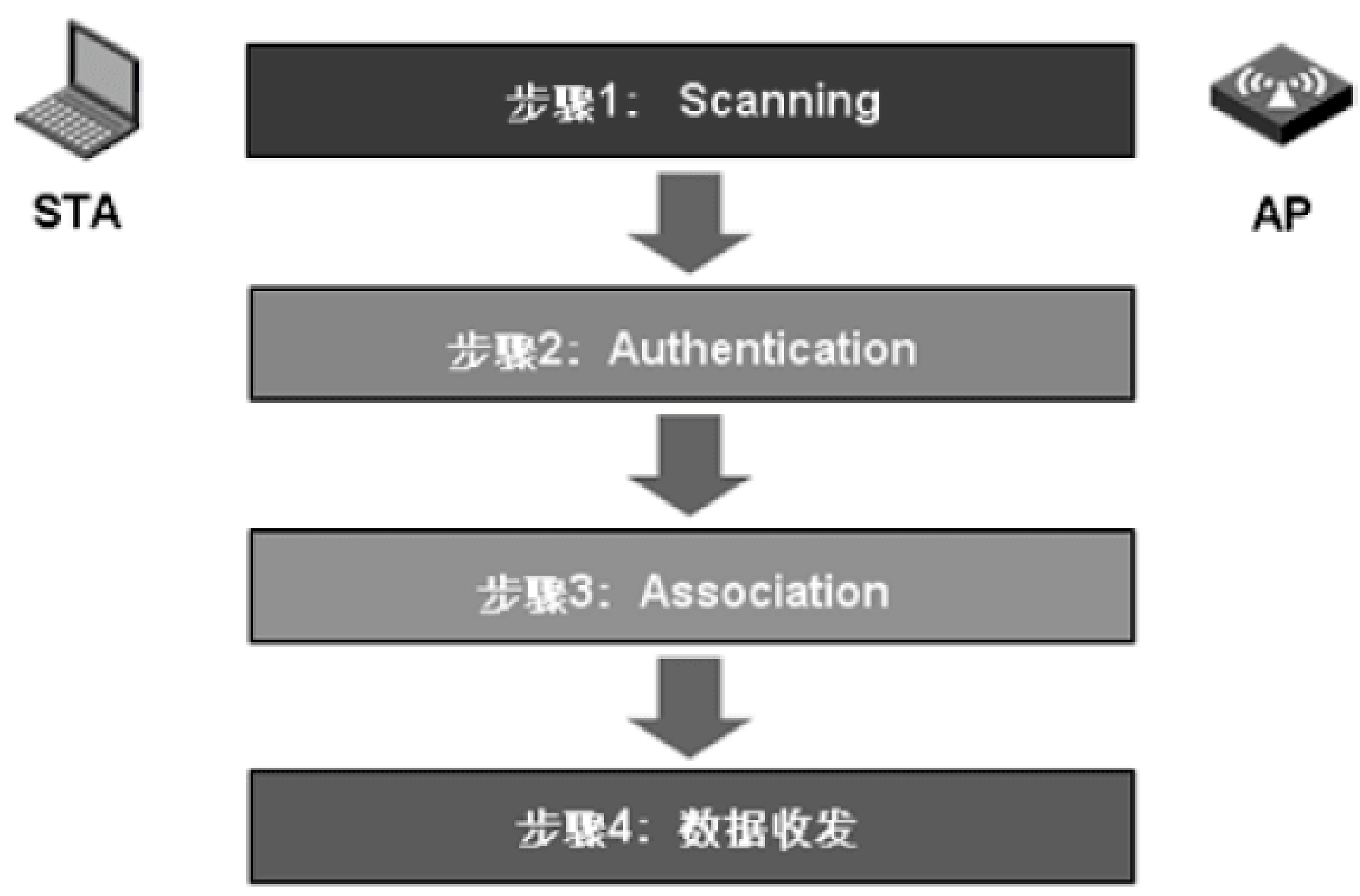


图 7-33 无线客户端接入 802.11 无线网络的过程

在排查无线终端关联失败故障的过程中，我们需要按照终端的关联过程依次排查，定位无线终端关联问题的思路如下。

首先，需要关注扫描过程，是否使用广播 SSID 方式，如果使用隐藏 SSID 方式则需要检查终端的设置，确保终端能够发现无线信号。

其次，确保认证报文交互成功，这里的认证只是简单的 AP 与 STA 间的 Authentication 报文交互，不是我们常说的 802.1x 或者 PSK 等高级认证。

最后，排查关联过程，常用的关联成功率也是与这一过程息息相关的，关联成功后则表示终端和 AP 可以进行正常的报文收发了，然后才能进行加密协商或者其他高级认证。

2. 流程图相关操作说明

(1) 当前 SSID 是否采用明文方式

常见的 SSID 又分为明文不加密方式和 WEP、WPA、WPA2 等加密方式，其中加密方式会受到终端的支持度、加密的配置等多种情况的影响。因此在排查问题时，我们需要先明确当前网络采用的方式。

(2) 新建明文 SSID，测试终端能否关联成功

当我们遇到终端接入故障时，可以新建一个明文、不加密的 SSID 进行测试。

```
[AC] wlan service-template 1 clear
[AC-wlan-st-1] ssid h3c
[AC-wlan-st-1] bind WLAN-ESS 1
[AC-wlan-st-1] service-template enable
```

```
[AC] interface WLAN-ESS 1
[AC-WLAN-ESS1] port access vlan 1(使用业务 vlan)
[AC] wlan ap ap model WA2210-AG
[AC-wlan-ap-ap] serial-id 210235A29EB092002600
[AC-wlan-ap-ap] radio 1
[AC-wlan-ap-ap-radio-1] service-template 1
[AC-wlan-ap-ap-radio-1] radio enable
```

(3) 判断网络信号强度是否达标

当终端在信号很弱的情况下，会导致无线链路非常不稳定。无线网路传输会对每个报文进行物理层的确认，在整个交互过程中，任何一方出现问题都会导致终端接入失败的现象。如何判断网络信号强度是否达标，共有以下几种方法可以尝试(测试信号强度低于－70dBm 为不达标)。

① 通过抓包工具 OmniPeek 等软件，分别在 AP 和 STA 处抓包查看对方信号强度。

② 通过信号分析工具黄马甲、频谱仪分析信号强度。

③ 通过信号勘测软件 Network Stumbler、inSSIDer 分析 AP 信号强度。

④ 将终端放到 AP 或天线附近测试能否关联，直接排除弱信号的情况，以便快速定位问题。

(4) 检查 AP 覆盖状态

① 判断当前 AP 是否使用最大发射功率，如果没有则需要将发射功率调整至最大值。

② 检查 AP 馈线各个接口是否松动，如有松动请及时修整。

③ 检查天线、AP 安装是否规范，请严格按照天线安装手册进行操作。

(5) 增强问题区域信号覆盖

在确定 AP 工作状态一切正常，但是问题区域信号仍然很弱时，可以通过调整天线、AP 的位置，或者在该区域增加 AP 的方式，改善问题区域信号覆盖强度。

(6) AP 关联用户数是否达到上限

当终端无法关联时，通过命令可以查看当前 AC 的日志，判断是否是当前 AP 的关联用户数达到配置上限。

命令：*display logbuffer*

例如：通过查看 logbuffer，可以确认终端关联失败是否是由于 AP 达到用户数上限。

```
[AC]display logbuffer
#Jan 2 08:43:04:974 2014 AC_2 WMAC/4/Station Association Fail: Station Assoc Fail:1.3.6.1.4.1.2011.10.2.75.3.2.0.4<h3cDot11StationAssocFailTrap> StaMac1:00:24:D7:9C:AF:4C StaMac2:00:24:D7:9C:AF:4C StaMac3:00:24:D7:9C:AF:4C Radioid:2 SSIDName:test Cause:2 Desc:Too Many Associations APID:210235A0T6C129000430
%Jan 2 08:43:05:020 2014 AC_2 WMAC/5/WMAC_TOO_MANY_ASSO_IN_RADIO: Client 0024-d79c-af4c failed to associate because of maximum clients in radio for APID 2, RadioId 2.
```

(7) 通过软件调整优化当前网络关联用户数

① 增加 idle-timeout 配置，时间为 10 分钟，来清除异常下线终端所占用的资源。

```
[AC]wlan ap ap
[AC-wlan-ap-ap]client idle-timeout 600
```

② 调整最大接入用户数限制，默认最大接入 64 个，不建议再调大。调整最大接入用户数

可以在 radio-policy 和 Service-template 模板下配置，两者都配置时取值小的生效。

(8) 通过硬件调整增加当前网络容量

如果用户数过多，超出 AP 容量上限，导致无法正常关联，则需要进行硬件整改，通过增加 AP 或者更换双频 AP 的方式解决关联用户数资源紧张问题。

(9) 是否存在备份 AC

检查现网是否设置 AC 备份。

(10) 检查主备 AC 的配置并修改一致

命令：*display current-configuration*

例如：通过命令查看主备 AC radio policy、射频口的配置是否一致。

```
[AC_2] display current-configuration
...
#
Wlan radio-policy radiopolicy1
beacon-interval 160
...
#
wlan ap ap model wa2100
serial-id 210235A22WB093002688
radio 1
service-template 1
client idle-timeout 300
radio-policy radiopolicy1
radio enable
#
...
```

命令：*display wlan rrm*

例如：通过命令查看 rrm 的配置，主备一定要保持一致。

```
[AC_2]display wlan rrm
                         RRM Configuration
---------------------------------------------------------------------------
 11a Configured Rates (Mbps)
   Mandatory               : 6, 12, 24
   Supported               : 9, 18, 36, 48, 54
   Multicast               : Auto
   Disabled                : -NA-
 11b Configured Rates (Mbps)
   Mandatory               : 1, 2
   Supported               : 5.5, 11
   Multicast               : Auto
   Disabled                : -NA-
 11g Configured Rates (Mbps)
   Mandatory               : 1, 2, 5.5, 11
   Supported               : 6, 9, 12, 18, 24, 36, 48, 54
```

可以通过文本比对软件将主备 AC 的配置进行比对，主备 AC 上关于 AP 的配置一定要改成一致的，否则会导致终端与 AC 的兼容出现故障，出现终端无法关联的现象。

(11) 检查 WIDS 黑白名单配置

查看 AC 是否配置了 WIDS 功能，如果配置了则需要注意如下情况。

① 配置黑名单中的用户，不能接入无线网路。

② 配置白名单后，非名单内的用户不能接入无线网络。

③ 同时配置黑白名单后，先检查白名单，只有白名单内的用户能接入，再检查黑名单，黑名单内的用户不能接入。

命令：*display current-configuration*

例如：通过命令查看是否有黑白名单相关的配置。

```
[AC_2] display current-configuration
#
static-blacklist mac-address 00aa-00aa-00aa
whitelist mac-address 00aa-00aa-00aa
#
```

（12）收集 log、trap 及 debugging 信息

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

① 当 AC 在线用户数少于或等于 100 时，建议用下面的命令收集信息并使用调试开关进行调试。

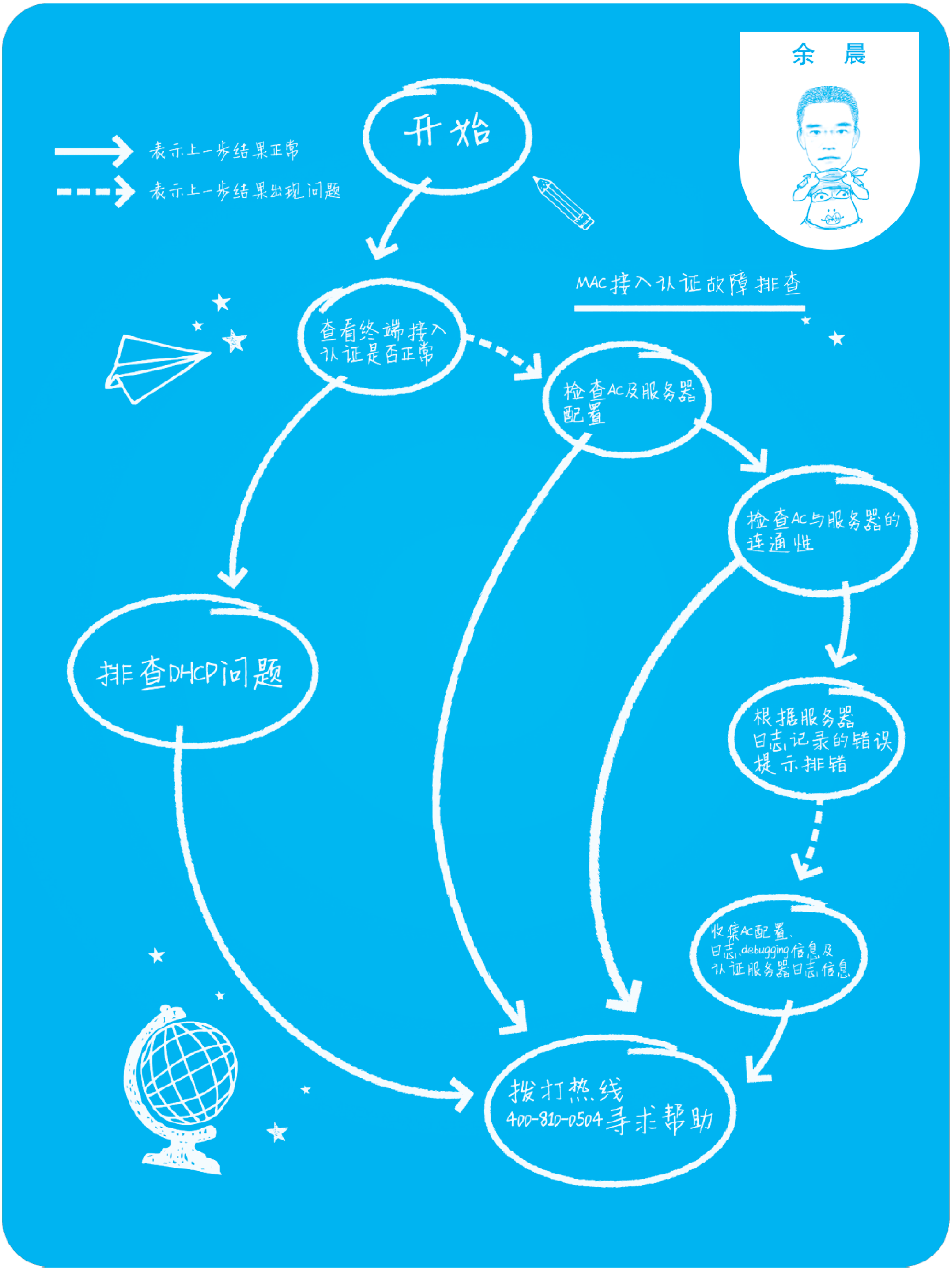
命令：*display logbuffer*

debugging wlan mac all

terminal monitor

terminal debugging

② 当 AC 在线用户数超过 100 时，建议等业务闲时关联用户数下降到 100 以下，再执行上述操作。


余 晨
表示上一步结果正常
表示上一步结果出现问题
开始
MAC接入认证故障排查
查看终端接入认证是否正常
检查AC及服务器配置
检查AC与服务器的连通性
根据服务器日志记录的错误提示排错
收集AC配置、日志、debugging信息及认证服务器日志信息
排查DHCP问题
拨打热线 400-810-0504寻求帮助

1. 开始

在 WLAN 网络中,链路接入部分和 MAC 地址认证看似是一个"强关联"的绑定关系,但是实际上 802.11 协议本身没有和 MAC 认证产生任何的关系,所以要充分认清楚链路接入和 MAC 认证的关系。

故障定位的思路如下。

首先,判断终端接入、获取地址是否正常。

其次,判断 AC 上、服务器上关于 MAC 认证的基本配置是否正常。

再次,判断 AC 与服务器的连通性是否正常。

最后,通过收集 AC 的 debugging 信息及服务器的认证日志信息,分析问题原因。

2. 流程图相关操作说明

(1) 查看终端接入认证是否正常

通过命令判断测试终端能否通过 MAC 认证。

命令: *display wlan client*

例如:通过命令查看终端信息,成功认证的终端就可以直接看到 User Name 为用户 MAC 地址的终端。

```
[AC]display wlan client
 Total Number of Clients              : 1
                                  Client Information
 SSID: MAC
-------------------------------------------------------------------------------------
MAC Address        User Name        APID/RID          IP Address            VLAN
-------------------------------------------------------------------------------------
4c8d-7979-7905     4c8d79797905     1    /2           192.168.1.9             1
```

(2) 排查 DHCP 问题

① 在 STA 上单击"开始"按钮→"运行"→输入"cmd"→按回车键,通过命令行查看终端地址获取情况。

命令: *ipconfig /all*

例如:通过命令查看,可以确认本机获取 IP 地址 192.168.1.8。

```
D:\>ipconfig /all
Ethernet adapter 无线网络连接:

Ethernet adapter 无线网络连接:

        Connection-specific DNS Suffix  . :
        Description. . . . . . : Intel(R) Centrino(R) Ultimate-N 6300 AGN
        Physical Address. . . . . . . . . : 00-24-D7-9C-AF-4C
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.8
```

② 如果终端没有成功获取地址，请检查参考命令手册检查 DHCP Server 配置是否符合规范。

(3) 检查 AC 及服务器配置

① 检查 AC 配置。

第一，明文及 WEP 加密方式的 WLAN 接入服务需要注意在 ESS 接口下选择正确模式。

```
interface WLAN-ESS 2
port-security port-mode mac-authentication
```

第二，WPA/RSN 方式的 WLAN 接入和 PSK+MAC 认证组合。

```
interface WLAN-ESS 3
port-security port-mode mac-and-psk
```

② 检查服务器配置。

一定要配置每一个“MAC 认证用户”的“在线数量限制”至少要设置为大于或者等于 2，如图 7-34 所示，对于 FAT AP 方式组网中建议设置为“6”。



图 7-34　“MAC 认证用户”在线数量限制设置

说明：如果“在线数量限制”设置为 1，可能会带来漫游不成功问题，甚至严重导致无线连接断开以及切换到别的 SSID 无线服务（当存在两个无线网络，而且都在无线网卡的自动连接列表中）。

(4) 检查 AC 与服务器的连通性

由于 AC 需要与 AAA 直接交互 Radius 协议报文，并使用指定的 IP 地址通信，即 Radius NAS-IP。因此，需要保证 AC 的 Radius NAS-IP 与 AAA 服务器路由可达。

① 测试 AC 与 AAA 的连通性，测试方法即 AC 带源 ping 服务器地址。

命令：*display radius scheme cmcc*

例如：通过命令查看 NAS-IP 地址。

```
[AC]display radius scheme cmcc
SchemeName   : cmcc
…
NAS-IP address                                  : 218.200.72.36
```

另外，注意排查网络中的防火墙等设备是否可能阻断 Radius 协议报文。

② 如果测试出现故障需要排查以下问题。

第一，检查 nas-ip 配置是否正确。

第二，通过逐级 ping 方式、抓包方式明确具体丢包的位置。

第三，在检查二层、三层设置是否符合规范，涉及具体协议可参考各协议的故障排查指导。

（5）根据服务器日志记录的错误提示排错

① 协调 Radius 侧，查看认证失败日志信息。

② 根据认证失败日志提示进行修改，例如：用户名密码设置错误等。

（6）收集 AC 配置、日志、debugging 信息及认证服务器日志信息

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

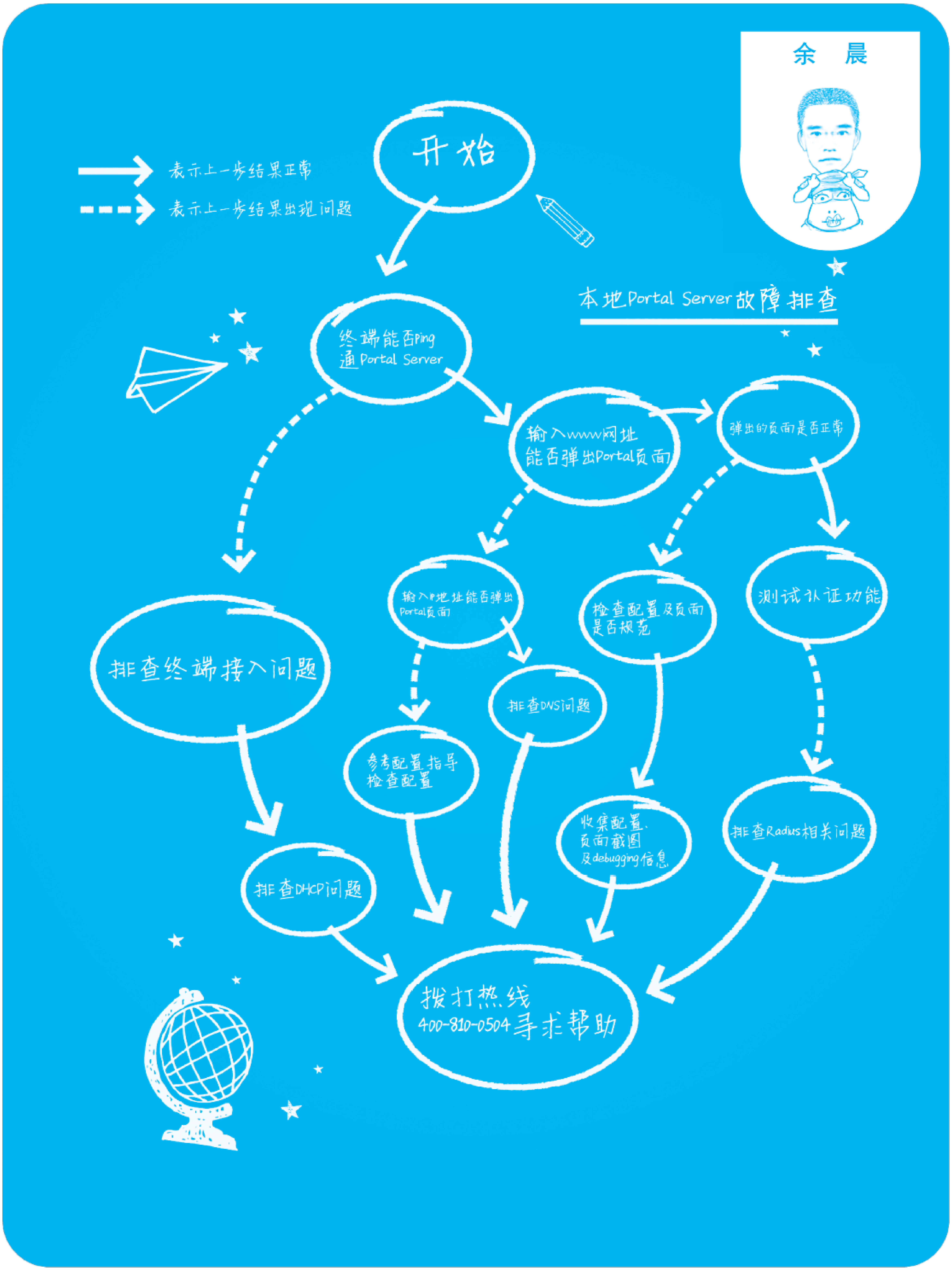
建议使用下面的调试开关进行调试。

① debugging wlan mac all（如果用户多的时候，不要 all 开关，可以逐条打开，例如 debugging wlan mac error→event→fsm→timer）。

② debugging port-security all：打开端口安全调试信息。

③ debugging mac-authentication event：打开 MAC 认证调试信息。

④ debugging radius packet：打开 Radius 的调试开关，该调试为可选。


余 晨
表示上一步结果正常
表示上一步结果出现问题
开始
本地Portal Server故障排查
终端能否ping通Portal Server
输入www网址能否弹出Portal页面
弹出的页面是否正常
输入IP地址能否弹出Portal页面
检查配置及页面是否规范
测试认证功能
排查终端接入问题
排查DNS问题
参考配置指导检查配置
收集配置、页面截图及debugging信息
排查Radius相关问题
排查DHCP问题
拨打热线 400-810-0504寻求帮助

1. 开始

Portal 认证凭借其简单方便、终端广泛支持、具备宣传效应等特点颇受市场欢迎，随着 Portal 认证的普及应用，客户对其要求也越来越多，定制页面的情况愈加普遍，由于在 AC 上定制页面存在诸多限制，因此需要按照标准仔细检查。

定位故障的思路如下。

首先，通过命令查看终端状态，判断接入、获取地址是否正常。

其次，判断终端到 Portal Server 的连通性及配置是否正常，判断定制页面是否符合规范。

再次，通过测试判断 AC 与 Radius 侧连通性及配置是否正常。

最后，收集 debugging 及配置信息分析。

2. 流程图相关操作说明

(1) 终端能否 ping 通 Portal Server

无线 Portal 认证属于三层认证，因此在认证成功之前需要能够访问 Portal Server，如果本地 Portal 出现故障，则需要先排除网络故障，建议通过 ping 测试与 Portal Server 的连通性(需要关闭禁 ping 功能)。

① 查看 IP 地址。

命令：*display portal server*

例如：通过命令查看 Portal Server 的 IP 地址。

```
[AC]display portal server
 Portal server:
  0)h3c:
     IP                : 192.168.1.3
```

② 在 STA 上单击“开始”按钮→“运行”→输入“cmd”→按回车键。

命令：*ping 192.168.1.3*

例如：通过 ping 操作检测与 Portal Server 的连通性。

```
D:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=20ms TTL=255
```

(2) 排查终端接入问题

① 可以在 AC 上通过命令查看用户的关联状态。

命令：*display wlan client mac-address 0024-d79c-af4c*

例如：通过命令查看无线用户有无关联 AC。

```
[AC]display wlan client mac-address 0024-d79c-af4c
 Total Number of Clients              : 1
                              Client Information
--------------------------------------------------------------------------------
MAC Address      User Name        APID/RID       IP Address          VLAN
--------------------------------------------------------------------------------
0024-d79c-af4c      -NA-          1    /1       192.168.1.8            1
```

② 如果终端没有正常接入，则需要排查无线接入问题，如图 7-35 所示。

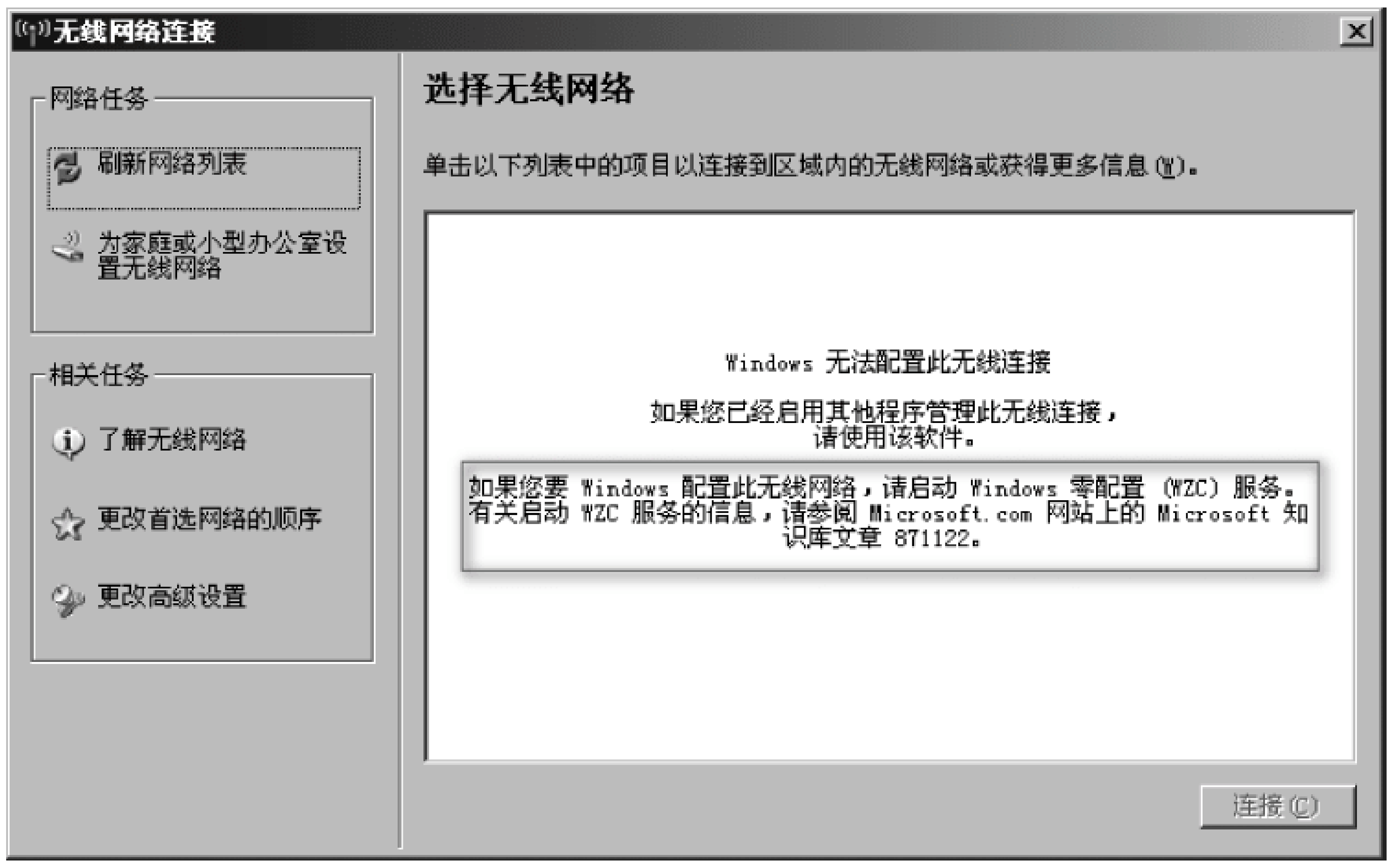


图 7-35　无线接入问题的排查

(a) 检测终端无线是否正常开关。

(b) 检测是否在终端服务中开启无线服务。

(c) 检测终端是否工作在正常的无线终端模式，如果错误的设置成 AP 模式则无法作为无线终端使用。

(d) 检测终端是否关联正确的 SSID。

(3) 排查 DHCP 问题

① 在 STA 上单击“开始”按钮→“运行”→输入“cmd”→按回车键，通过命令行查看终端地址获取情况。

命令：*ipconfig /all*

例如：通过命令查看，可以确认本机获取 IP 地址 192.168.1.8。

```
D:\>ipconfig /all
Ethernet adapter 无线网络连接:

Ethernet adapter 无线网络连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) Centrino(R) Ultimate-N 6300
 AGN
        Physical Address. . . . . . . . . : 00-24-D7-9C-AF-4C
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.8
```

② 排查 DHCP 问题。

请参考云图《IP 业务——DHCP 排查模块》。

(4) 输入 www 网址能否弹出 Portal 页面

① 操作方式：终端打开浏览器，在浏览器地址栏输入任意 IP 地址(如 www.baidu.com)，正常情况下 AC 会对终端的访问进行 TCP 仿冒，将终端重定向强制使其访问 Portal Server 的认证页面。

② 终端成功访问 Portal 页面需要具备的条件如下。

(a) 终端报文能顺利送到 AC。

(b) 使用 www 网址方式，终端必须可以正常的进行 DNS 解析，直接输入 IP 地址则不需要进行这一步操作。

(c) 终端具备触发 AC 的 http 重定向的条件，且无线链路必须已经建立并能正常通信。

(d) 终端和 Portal 服务器的路由必须可达。

(5) 输入 IP 地址能否弹出 Portal 页面

操作方式：终端打开浏览器，在浏览器地址栏输入任意 IP 地址(如 1.1.1.1)，正常情况下 AC 会对终端的访问进行 TCP 仿冒，将终端重定向强制使其访问 Portal Server 的认证页面。

(6) 排查 DNS 问题

① 在 STA 上单击“开始”按钮→“运行”→输入“cmd”→按回车键，通过命令行查看终端地址获取情况。

命令：*ipconfig /all*

例如：通过命令查看，可以确认本机获取的 DNS 地址为 192.168.1.3。

```
D:\>ipconfig /all
Ethernet adapter 无线网络连接:

Ethernet adapter 无线网络连接:
...
DNS Servers . . . . . . . . . . . : 192.168.1.3
```

② 在 STA 上单击“开始”按钮→“运行”→输入“cmd”→按回车键，然后尝试 ping 上文查看到的 DNS 地址。

命令：*ping 192.168.1.3*

例如：通过 ping 操作检测与 DNS Server 的连通性。

```
D:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=20ms TTL=255
```

③ 排查 DNS 问题。

(a) 检查 free-rule 的配置，因为 Portal 只对 IP 进行重定向，因此使用 www 网址方式访问时，必须先做 DNS 解析，所以在认证之前终端就必须保证与 DNS Server 之间是互通的。

命令：*display portal free-rule*

例如：通过命令可以查看当前 free rule 里面有没有正确放通 DNS Server 地址。

```
[AC]display portal free-rule
 Rule-Number   0:
...
 Destination:
   IP          : 192.168.1.3
   Mask        : 255.255.255.255
```

(b) 检查 DNS 解析是否正常，通过抓包可以查看 DNS 有没有解析 IP 地址。

(c) 如果无法正常解析,则需要检查二层、三层设置是否符合规范,涉及具体协议可参考各协议的排障指导。

(7) 参考配置指导检查配置

Portal 的基本配置需要先做核实。

命令:*display current-configuration | include portal*

例如:主要查看 Portal Server 的配置是否正确,包括绑定的 SSID 是否正确,zip 文件是否正确,接口下是否开启 Portal 功能。

```
<AC>display current-configuration | include portal
 portal server h3c ip 192.168.1.3 server-type imc
 portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
 portal local-server http
 portal local-server bind ssid h3c-portal file http.zip
 portal server h3c method direct
```

(8) 弹出的页面是否正常

① 通过现场判断,弹出的页面是否为预期页面,如果出现异常请参考下一步排障指导。

② AC 版本文件中包涵一个内置的 Portal 页面文件,如果希望改动原有页面则需要自己定制,当定制页面无法弹出时会弹出内置页面。

(9) 检查配置及页面是否规范

特殊配置检查。

命令:*display current-configuration | include portal*

例如:主要查看 Portal Server 的配置是否正确,包括绑定的 SSID 是否正确,zip 文件是否正确,接口下是否开启 Portal 功能。

```
<AC>display current-configuration | include portal
 portal server h3c ip 192.168.1.3 server-type imc
 portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
 portal local-server http
 portal local-server bind ssid h3c-portal file http.zip
 portal server h3c method direct
```

定制页面检查。

由于 Portal 定制页面需要放在 AC 上面,因此需要遵循 AC 的一些定制需求。实际使用中经常出现 AC 推送 Portal 页面不成功,文件正确但推出的页面总是版本自带的页面,这里简单总结几点配置 AC 推送 Portal 页面时需要注意的问题。

① Portal 页面文件压缩格式必须为 zip。

② 压缩后的 zip 文件大小不能超过 500KB。

③ 每个单独页面(包括单个主索引页面文件及其页面元素)压缩前的文件大小不能超过 50KB。

④ 尤其注意在修改页面文件后,压缩文件时,一定保证压缩的文件解压时的目录只有一级,如图 7-36 所示。

如果压缩后的文件解压时出现多级目录,则 AC 推送页面会失败,但实际上文件并没有损坏或更改错误,如图 7-37 所示。



图 7-36 压缩文件解压时的目录只有一个



图 7-37 压缩文件解压时出现多级目录

建议压缩文件时，进入文件夹后，全选文件，然后压缩，保证压缩后的目录只有一级，如图 7-38 所示。

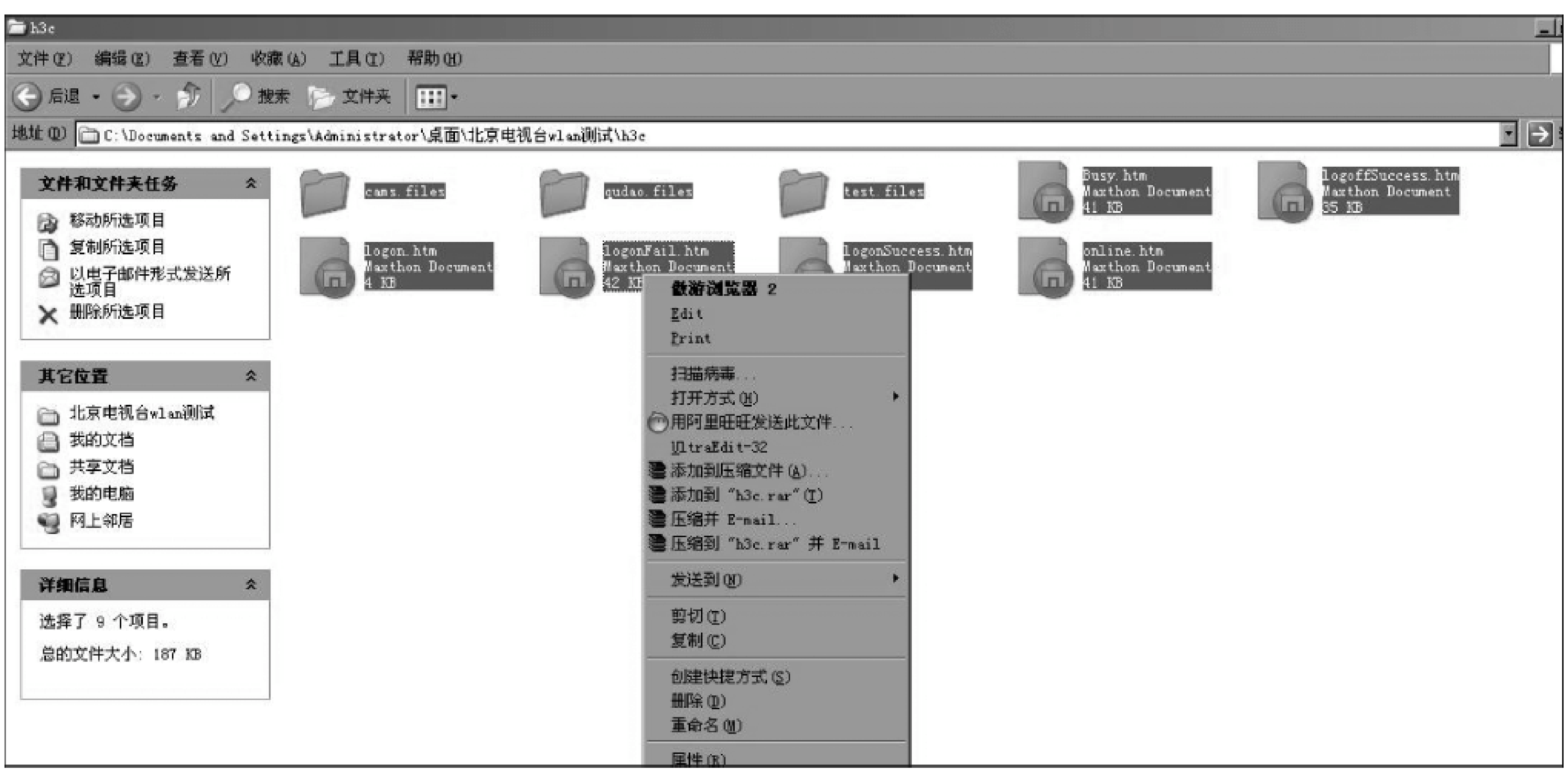


图 7-38 保证文件压缩后的目录只有一级

不要直接选择文件夹进行压缩，如图 7-39 所示。



图 7-39　直接选择文件进行压缩

⑤ 需要注意，修改完文件后需要重新导入 AC，并且需要重新配置 Portal 认证。

⑥ 详细文档见 KMS-23677。

(10) 收集配置、页面截图及 debugging 信息

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

请收集以下信息。

命令：

```
<AC>display current-configuration
<AC>debugging portal all interface Vlan-interface 2
<AC>debugging portal error
<AC>debugging portal server
<AC>debugging portal tcp-cheat
<AC>terminal monitor
<AC>terminal debugging
```

说明：以上信息必须同时开启。

(11) 测试认证功能

通过上文排查后可以正常的弹出 Portal 登录页面，此时需要输入用户名、密码测试，如果提示认证失败、超时等信息，则可以判断为 Radius 相关问题。

(12) 排查 Radius 相关问题

由于 AC 需要与 AAA 直接交互 Radius 协议报文，并使用指定的 IP 地址通信，即 Radius nas-ip。因此需要保证 AC 的 Radius nas-ip 与 AAA 服务器路由可达。

① 测试 AC 与 AAA 的连通性，测试方法即 AC 带源 ping 服务器地址。

命令：*display radius scheme cmcc*

例如：通过命令查看 nas-ip 地址。

```
[AC]display radius scheme cmcc
SchemeName   : cmcc
…
NAS-IP address                                        : 218.200.72.36
```

另外，注意排查网络中的防火墙等设备是否可能阻断 Radius 协议报文。

② 如果测试出现故障需要排查以下问题。

(a) 检查 nas-ip 配置是否正确。

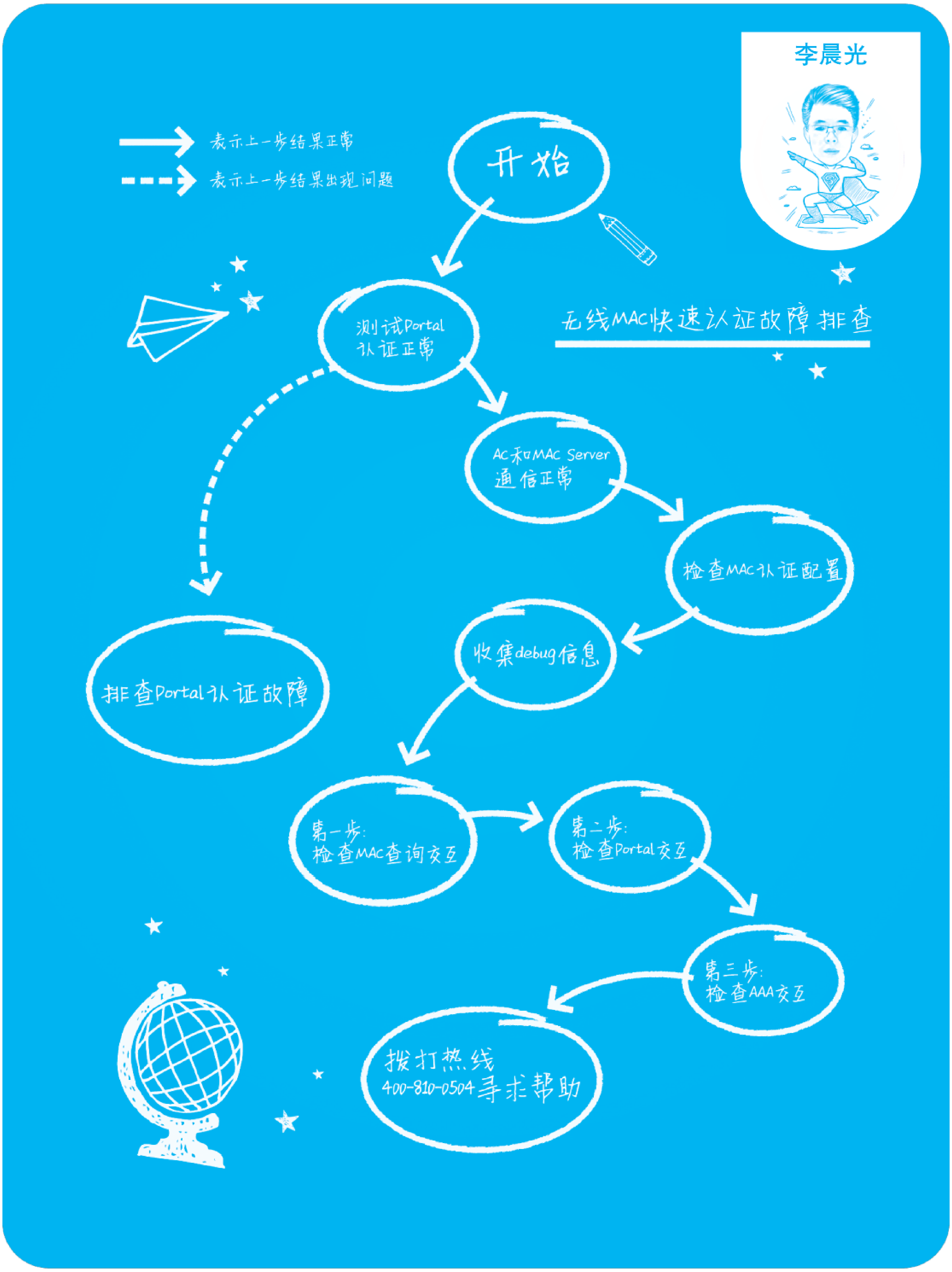
(b) 通过逐级 ping 方式、抓包方式明确具体丢包的位置。

(c) 在检查二层、三层设置是否符合规范，涉及具体协议可参考各协议的排障指导。

③ 收集 debugging 信息。

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

debugging Radius packet：打开 Radius 的调试开关，该调试为可选。


李晨光
表示上一步结果正常
表示上一步结果出现问题
无线MAC快速认证故障排查
开始
测试Portal认证正常
AC和MAC Server通信正常
检查MAC认证配置
收集debug信息
排查Portal认证故障
第一步：检查MAC查询交互
第二步：检查Portal交互
第三步：检查AAA交互
拨打热线 400-810-0504寻求帮助

1. 开始

无线 MAC 快速认证也叫智能终端 MAC 快速认证或无感知认证。

无线 MAC 快速认证是在普通的 Portal 认证架构新增了一个 MAC 绑定查询服务器。并对原 Portal 认证流程做了改动，在重定向之前增加了一个 MAC 查询的步骤，即用户流量到达 AC 后并不立刻触发 Portal 重定向，而是由 AC 先和 MAC 绑定服务器完成 MAC 绑定查询，只有未绑定 MAC 的用户才触发 Portal 重定向，进行普通认证流程。对于已经绑定 MAC 的用户，AC 不会触发重定向功能，而是等待 Portal Server 或 MAC 绑定服务器(此时充当 Portal Server)向 AC 发起针对该绑定用户的 Portal 认证，此过程中用户并不需要介入，因此也称为无感知认证。

所以定位故障的思路是：首先确保普通的 Portal 认证业务正常，再检查 MAC 绑定查询的交互过程。

2. 流程图相关操作说明

(1) 测试 Portal(Web)认证正常

MAC 快速认证是以 Web 方式的 Portal 认证流程为基础，所以普通 Portal 认证业务正常是 MAC 快速认证的前提。

测试方法：使用未绑定 MAC 的终端进行常规 Portal 业务测试；或者在 AC 上取消 MAC 快速认证功能，测试常规 Portal 业务。

(2) 排查 Portal 认证故障

如果常规 Portal 业务存在故障，则按云图——《无线 Portal 认证故障排查》标准流程图处理。

(3) AC 和 MAC Server 通信正常

AC 需要和 MAC Server 完成对用户 MAC 绑定的查询，因此 AC 和 MAC Server 的路由可达也是 MAC 快速认证成功的前提之一。

检查方法：AC 带 NAS-IP 源地址 ping MAC Server 服务器地址。另外，注意排查网络中的防火墙等设备是否可能阻断 Portal 协议报文。

关于 Portal NAS-IP：AC 的 Portal NAS-IP 可以在三层 Interface-VLAN 口指定，如果未指定，默认以三层 Interface-VLAN 口地址作为 NAS-IP。

```
<H3C>display current-configuration
#
interface Vlan-interface1102
 ip address 211.140.8.129 255.255.255.0
 portal server cmcc-jituan method direct
 portal domain jituan
 portal mac-trigger enable period300 threshold 10240
 portal nas-ip 218.xx.xx.36
 access-user detect type arp retransmit 5 interval 10
#
```

如果 AC Portal NAS-IP 地址到服务器 ping 不通，则需要排查路由互通。

(4) 检查 MAC 认证配置

检查 AC 与 MAC Server 通信的 IP、端口号配置，以及流量触发门限配置。

说明：在 AC 上要将 MAC Server 同时配置为 Portal Server，即允许 MAC Server 直接向 AC 发起 Portal 认证。

```
<H3C>display current-configuration
#
portal mac-trigger server ip 211.xx.xx.57 port 50100
portalserver mac-server-xxx ip 211.xx.xx.57
#
interface Vlan-interface1102
 ip address 211.140.8.129 255.255.255.0
 portal server cmcc-jituan method direct
 portal domain jituan
 portal mac-trigger enable period300 threshold 10240
 portal nas-ip 218.xx.xx.36
 access-user detect type arp retransmit 5 interval 10
```

(5) 收集 debug 信息

收集 Portal 和 Radius 的调试信息，注意：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

命令：

```
<AC> debugging portal packet interface xxx
<AC> debugging radius packet
```

可以对照 MAC 快速认证的原理流程来分析 debug 信息，基本过程简述如下。

① AC 向 MAC Server 发送 Portal Type：48(0x30)的查询报文。

② MAC Server 回应 Portal Type：49(0x31)的应答报文，ErrCode 为 0 表示 MAC 已绑定，ErrCode 为 1 表示 MAC 未绑定。

③ Portal Server/MAC Server 向 AC 发起 Portal 认证，用于认证的用户名\密码为 MAC Server 从 AAA 同步过来的账号信息。

④ AC 向 Radius 服务器发起 AAA 认证。

⑤ 认证通过后用户能访问网络。

详细 debug 信息的分析如下。

(6) 检查 MAC 查询交互

```
 * Apr 27 13:54:57:173 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Send REQ-MAC-BIND for the 1th time.
 * Apr 27 13:54:57:174 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal send packet length:48
Portal packet head:
Type:48 SN:16130 ReqId:0     AttrNum:3   ErrCode:0   UserIP:10.197.58.100
   Portal packet attribute list:
      [ 11 Session-ID           ] [  8] [34e0cfd601e8]
      [ 10 BAS-IP               ] [  6] [111.17.233.65]
      [ 48 Nas-ID               ] [ 18] [7178053153100460]
   Portal raw packet:
```

```
  01 30 00 00 3f 02 00 00 0a c5 3a 64 00 00 00 03
  0b 08 34 e0 cf d6 01 e8 0a 06 6f 11 e9 41 30 12
  37 31 37 38 30 35 33 31 35 33 31 30 30 34 36 30

* Apr 27 13:54:57:327 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:16
  Portal check packet OK
Portal packet head:
Type:49 SN:16130 ReqId:0    AttrNum:0   ErrCode:0   UserIP:10.197.58.100
  Portal packet attribute list:
   NULL
  Portal raw packet:
   01 31 00 00 3f 02 00 00 0a c5 3a 64 00 00 00 00

* Apr 27 13:54:57:328 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Receive ACK-MAC-BIND, MAC:34E0-CFD6-01E8, IP:0xac53a64, code:0
```

正常的 debug 情况如上，如果服务器回应 Type：49 号报文，且 ErrCode 为 0，说明 MAC 查询成功；若 ErrCode 为 1，说明 MAC 查询失败；如果服务器没有 Type：49 号报文回应，则说明报文在网络侧丢失或者服务器未响应，需要排查路由或者服务器侧配置。

（7）检查 Portal 交互

```
* Apr 27 13:54:57:370 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:16
  Portal check packet OK
Portal packet head:
Type:1   SN:27    ReqId:0     AttrNum:0   ErrCode:0   UserIP:10.197.58.100
  Portal packet attribute list:
   NULL
  Portal raw packet:
   01 01 00 00 00 1b 00 00 0a c5 3a 64 00 00 00 00

* Apr 27 13:54:57:370 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal send packet length:34
Portal packet head:
Type:2   SN:27    ReqId:37438 AttrNum:1   ErrCode:0   UserIP:10.197.58.100
  Portal packet attribute list:
   [  3 Challenge          ] [ 18] [a786bd4f07f6e3725ec7880e094c716e]
  Portal raw packet:
   01 02 00 00 00 1b 92 3e 0a c5 3a 64 00 00 00 01
   03 12 a7 86 bd 4f 07 f6 e3 72 5e c7 88 0e 09 4c
   71 6e

* Apr 27 13:54:57:372 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:64
  Portal check packet OK
Portal packet head:
Type:3   SN:27    ReqId:37438 AttrNum:2   ErrCode:0   UserIP:10.197.58.100
  Portal packet attribute list:
   [  1 UserName           ] [ 30] [15194159123@wlan-moni-jituan]
   [  4 ChapPassWord       ] [ 18] [b28071c504a0ad64ffc533a69a8887ba]
  Portal raw packet:
   01 03 00 00 00 1b 92 3e 0a c5 3a 64 00 00 00 02
```

```
01 1e 31 35 31 39 34 31 35 39 31 32 33 40 77 6c
61 6e 2d 6d 6f 6e 69 2d 6a 69 74 75 61 6e 04 12
b2 80 71 c5 04 a0 ad 64 ff c5 33 a6 9a 88 87 ba
```

MAC 查询成功后，表示用户已绑定 MAC，则 AC 会等待 Portal Server/MAC Server 向设备发起 Portal 认证。其中共有 3 个报文交互，Portal Type：1(REQ_CHALLENGE)、Type：2(ACK_CHALLENGE)、Type：3(REQ_AUTH)。

这之后就是等待 AC 完成 AAA 交互。

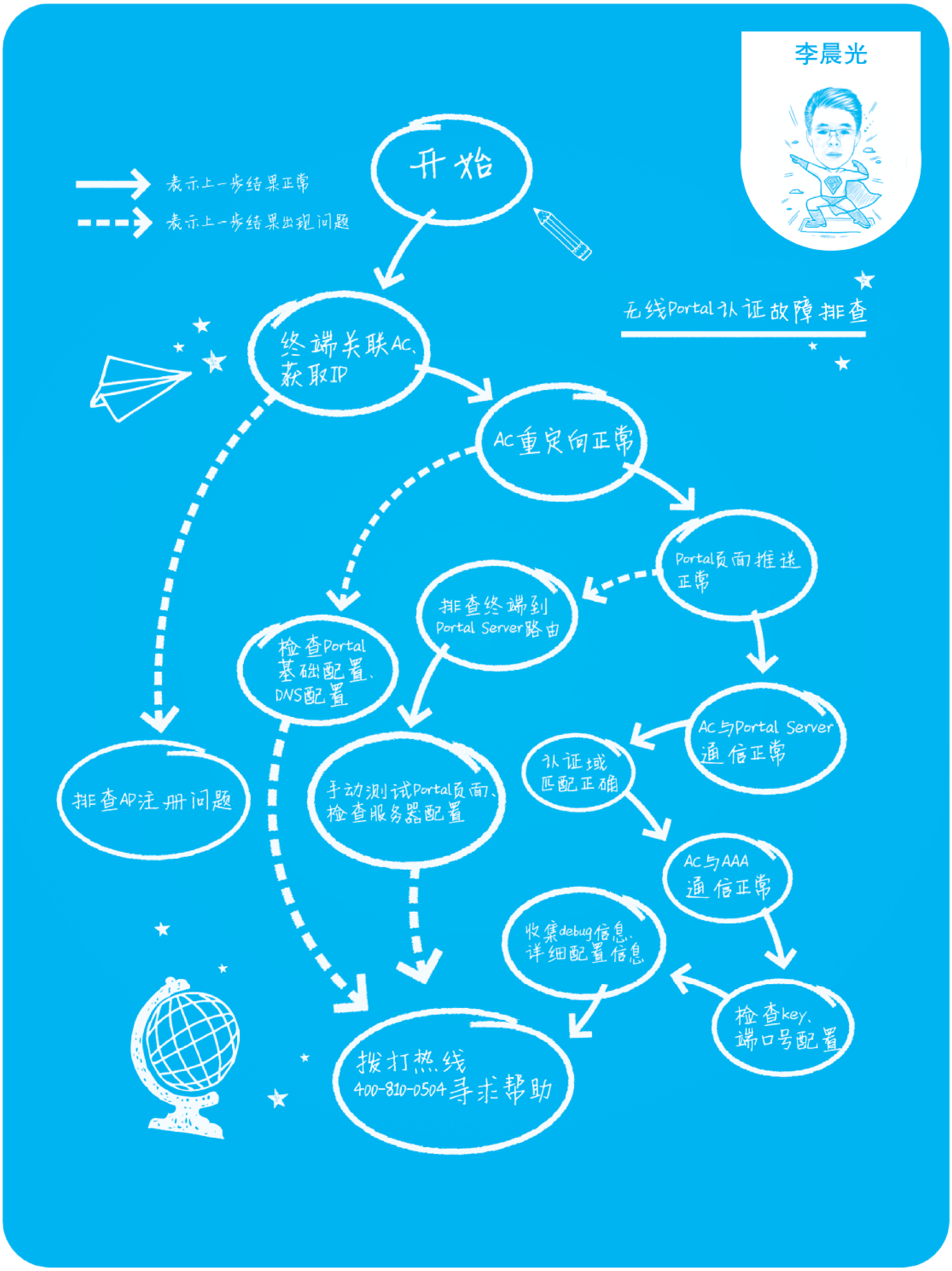
(8) 检查 AAA 交互

```
* Apr 27 13:54:57:380 2013 SDJN-WLAN-AC26-HSWX6108-AC1 RDS/7/DEBUG: Send: IP=[211.137.185.105], UserIndex=[3108], ID=[175], RetryTimes=[0], Code=[1], Length=[260]

* Apr 27 13:54:57:396 2013 SDJN-WLAN-AC26-HSWX6108-AC1 RDS/7/DEBUG: Receive: IP=[211.137.185.105], Code=[2], Length=[106]
```

此过程为标准的 Radius 认证流程，Code=[1]为认证请求报文，Code=[2]为认证成功响应。

如果此过程交互成功，即代表 MAC 认证最终完成，用户可以访问网络。如果收到的服务器回应报文不是 Code=[2]，而是 Code=[3]认证拒绝报文，则代表 AAA 拒绝用户登录，报文详细解析中一般会携带拒绝的原因。


李晨光
无线Portal认证故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
终端关联AC、获取IP
AC重定向正常
Portal页面推送正常
AC与Portal Server通信正常
认证域匹配正确
AC与AAA通信正常
检查key、端口号配置
收集debug信息、详细配置信息
排查终端到Portal Server路由
检查Portal基础配置、DNS配置
手动测试Portal页面、检查服务器配置
排查AP注册问题
拨打热线 400-810-0504寻求帮助

07 无线产品 > 7.4 认证 > 7.4.4 无线 Portal 认证故障排查 > 步骤详解

1. 开始

本流程图针对如下组网架构：AC 或 IAG(本文以 AC 统一称谓)作为 Portal 认证点，配合远程 Portal Server 做无线 Portal 认证。

无线 Portal 认证流程简述：首先，终端和 Portal Server 通过 http 协议建立连接，通过 Web 交互方式上传用户名、密码；其次，Portal Server 通过 Portal 协议向 AC 发起认证；最后，AC 通过 Radius 协议向 AAA 服务器验证用户身份。认证成功后 AC 对终端准予放行。

所以定位故障的思路是：首先确保终端和 Portal 服务器的 Web 通信正常，其次检查 Portal 和 AAA 交互的过程。

2. 流程图相关操作说明

(1) 终端关联 AC、获取 IP

无线 Portal 认证是根据用户 IP 地址来标识用户的，所以 Portal 认证前用户必须已经关联 AC 并获取到有效的 IP 地址。

可以在 AC 上通过命令查看用户的关联状态。

命令：*display wlan client*

例如：通过命令查看无线用户有无关联 AC。

```
<AC>display wlan client
 Total Number of Clients              : 2
                           Client Information
 SSID: wlan-telnet
----------------------------------------------------------------------------
MACAddress      User Name       APID/RID IP Address                  VLAN
----------------------------------------------------------------------------
2477-038f-8e68 -NA-              2    /1    192.168.3.6              999
2477-0391-2060 -NA-              2    /1    192.168.3.3              999
----------------------------------------------------------------------------
```

(2) 排查 AP 注册问题

① 确保终端接收的信号在 -75dBm 以上，保证正常关联。例如：Windows 7 客户端显示的无线信号强度在 3 格以上，如图 7-40 所示。



图 7-40　Windows 7 客户端无线信号强度显示

② 确保终端通过 DHCP 获取正确的 IP 地址。为了排查 DHCP 的故障点，可以在 AC 上起三层用户 VLAN 接口，配置动态获取 IP 地址，观察 AC 能否获取正确 IP 地址。如果 AC 都无法获取 IP 地址，需要排查有线侧 DHCP Server 的配置和二层 VLAN 互通性。

命令：*ip address dhcp-alloc*

例如：在业务 VLAN 999 上配置动态获取 IP 地址。

```
[AC-Vlan-interface999]ip address dhcp-alloc
```

命令：*display ip interface brief*

```
<AC>display ip interface brief
 * down: administratively down
(s): spoofing
Interface              Physical   Protocol   IP Address      Description
M-GE1/0/0              down       down       unassigned      M-Gigabit...
Vlan99                 up         up         117.21.55.244   mananger_...
Vlan999                up         up         192.168.3.6     Vlan-inte...
```

(3) AC 重定向正常

Portal 的业务模式是用户在认证前访问的任何页面都会被 AC 重定向到 Portal 认证主页，AC 重定向成功的直观表现是浏览器上能看到地址栏自动跳转为 Portal 认证 URL。

例如：终端浏览器地址栏自动跳转到 Portal 认证 URL，如图 7-41 所示。



图 7-41　终端浏览器地址栏

原理解析：用户在通过 Portal 认证前，向任意地址发出 http 请求。AC 会阻断并仿冒该地址和终端建立 http 连接。AC 再通过 http 重定向功能，将终端的访问请求重定向至 Portal Server 的认证主页。之后终端浏览器地址栏开始跳转并 Load 认证页面。

AC 重定向功能是否生效可以通过在终端 PC 上抓包确定。

例如：PC 上通过 Wireshark 抓包信息观察 AC 重定向，有“HTTP/1.1 302 Moved Temporarily”报文，如图 7-42 所示。

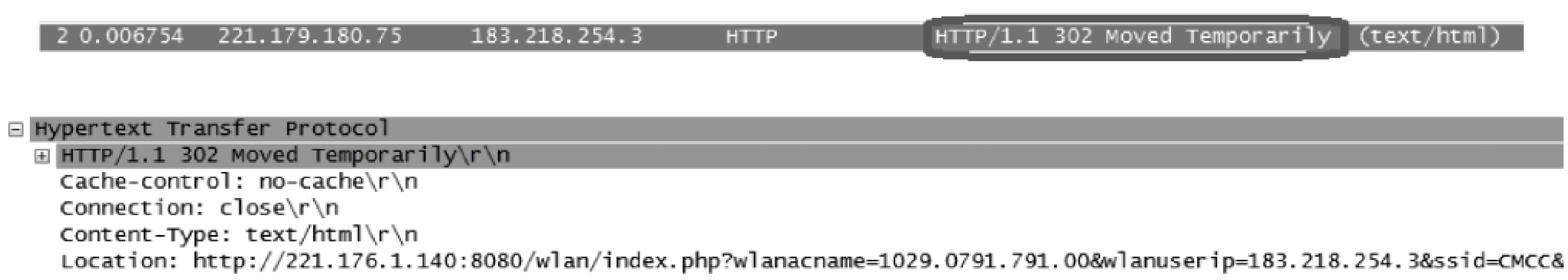


图 7-42　Wireshark 抓包信息

(4) 检查 Portal 基础配置、DNS 配置

检查 AC 全局 Portal 配置，在接口下使能 Portal 服务，并添加 DNS free-rule 放通规则。

命令：*display current-configuration*

```
<H3C>display current-configuration
#
portal server cmcc ip 10.202.164.10 url http://10.202.164.10:8080/portal/ server-type cmcc
portal free-rule 1 source any destination ip 211.137.58.20 mask 255.255.255.255
#
interface Vlan-interface1102
 description GateWay_of_CMCC
 ip address 192.168.3.254 255.255.224.0
 portal server cmcc method direct
 portal nas-id 3999071627000460
```

```
  portal nas-port-type wireless
  portalnas-ip 218.xx.xx.36
  access-user detect type arp retransmit 5 interval 10
#
```

原理解析：AC 完成重定向需要具备的条件如下。

① 浏览器访问的域名必须先能被 DNS 成功解析。

② AC 在用户三层 VLAN 接口上使能 Portal 功能。

常见错误：终端在浏览器上使用域名方式无法被重定向至 Portal 页面，但使用 IP 地址可以。原因：DNS 无法解析，DHCP Server 未配置 DNS 或者 DNS 服务器不可用（如未被 portal free-rule 放通）。

（5）Portal 页面推送正常

终端浏览器能成功 Load 完整的 Portal 主页。

（6）排查终端到 Portal Server 路由

如果 Portal 页面无法打开，或者打开不完整，可能的原因为：AC 到 Server 路由不可达、丢包，或者 Portal 服务器配置错误。

① 排查终端到 Portal Server 的路由，可以通过终端 ping Portal 服务器来测试，如图 7-43 所示。

命令：*ping －l 1500 x.x.x.x*



图 7-43　终端到 Portal Server 的路由排查

② 当终端到服务器能 ping 通，但丢包超过 3%时，还需要同时排查无线链路质量问题。无线丢包问题排查参考云图《无线空口丢包问题处理》标准流程图处理。

（7）手动测试 Portal 页面、检查服务器配置

在确定终端到 Portal Server 路由已经可达的前提下，如终端仍无法打开 Portal 页面。则可能是服务器故障，或者终端浏览器故障。

建议更换一台测试电脑，手工输入 Portal Server 的 URL，如仍无法打开页面，则基本确定是 Portal Server 故障。需要排查 Portal Server 配置，如图 7-44 所示。

（8）AC 与 Portal Server 通信正常

AC 需要与 Portal Server 直接交互 Portal 协议报文，并使用指定的 IP 地址通信，即 Portal nas-ip。因此需要保证 AC 的 Portal nas-ip 与 Portal 服务器路由可达。

检查方法：AC 带 nas-ip 源地址 ping 服务器。另外，注意排查网络中的防火墙等设备是否可能阻断 Portal 协议报文。



图 7-44　无法打开 Portal 页面

关于 Portal nas-ip：AC 的 Portal nas-ip 可以在三层 interface-vlan 口指定，如果未指定，默认以三层 interface-vlan 口接口地址作为 nas-ip。

```
<H3C>display current-configuration
#
interface Vlan-interface1102
 description GateWay_of_CMCC
 ip address192.168.3.254 255.255.224.0
 portal server cmcc method direct
 portal nas-id 3999071627000460
 portal nas-port-type wireless
 portalnas-ip 218.xx.xx.36
 access-user detect type arp retransmit 5 interval 10
#
```

说明：在中国移动的 WLAN Portal 认证过程中，AC 的 nas-ip 是与局数据“AC_NAME”一一对应的。AC 上除了 nas-ip，还需要配置正确的“AC_NAME”参数。该参数需要向集团申请，称为“局数据”。

命令：*portal device-id 0062.xx.xx.00*

```
<H3C>display current-configuration
#
portal server cmcc ip 221.x.x.140 url http://221.x.x.140:8080/index.php server-type cmcc
portal free-rule 1 source any destination ip 211.137.58.20 mask 255.255.255.255
portal device-id 0062.xx.xx.00
#
```

(9) 认证域匹配正确

AC 需要选择认证策略，即针对用户匹配认证域 Domain。设备上有多个地方可能配置认证域信息，各种匹配有先后顺序之别。

优先级顺序如下(由高到低)。

① 全局根据 SSID 和 AP 热点指定使用的 Portal 认证域。

命令：*portal wlan ssid xxxx server yyyy domain zzzz*

```
<H3C>display current-configuration
#
portal wlan ssid CMCC server cmcc-portal domain cmcc-wlan
```

② 三层接口下强制 Portal 认证域。

命令：*portal domain zzzz*

```
<H3C>display current-configuration
#
interface Vlan-interface1102
portal domain cmcc-wlan
```

③ 用户名携带的"@后缀名"匹配域。

④ 全局 domain default。

命令：*domain default zzzz*

```
<H3C>display current-configuration
#
domain default cmcc-wlan
```

说明：如果①、②、③按优先级顺序匹配过程中出现指定的域在 AC 全局并没有定义，则走全局 domain if-unknown 配置；如果 domain if-unknown 没有配置则认证失败。

命令：*domain if-unknown zzzz*

```
<H3C>display current-configuration
#
domain if-unknown cmcc-wlan
```

(10) AC 与 AAA 通信正常

AC 需要与 AAA 直接交互 Radius 协议报文，并使用指定的 IP 地址通信，即 Radius nas-ip。因此需要保证 AC 的 Radius nas-ip 与 AAA 服务器路由可达。

检查方法：AC 带 NAS-IP 源地址 ping 服务器。另外，注意排查网络中的防火墙等设备是否可能阻断 Radius 协议报文。

关于 Radius nas-ip：AC 可以在 Radius 策略中指定 Radius NAS-IP。

命令：*nas-ip x.x.x.x*

```
<H3C>display current-configuration
#
radius scheme cmcc
 server-type extended
 primary authentication 221.176.1.138 1645
 primary accounting 221.176.1.138 1646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 user-name-format keep-original
 nas-ip 218.xx.xx.36
 retry stop-accounting 10
#
```

如果 AC Radius NAS-IP 地址到服务器 ping 不通，则需要排查路由互通。

(11) 检查 key、端口号配置

检查 AC 与 Portal、AAA 通信的 key、端口号配置。服务器侧的配置也需要同步检查。

```
<H3C>display current-configuration
#
portal serverimc ip 10.0.0.1 key h3c url http://10.0.0.1/portal
#
radius scheme cmcc
 server-type extended
 primary authentication 221.176.1.138 1645
 primary accounting 221.176.1.138 1646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 user-name-format keep-original
 nas-ip 218.xx.xx.36
 retry stop-accounting 10
#
```

当 Radius key 配置错误时,设备上 debug 信息也能看出来。

命令:*debugging radius packet*

```
<H3C> debugging radius packet
…
*Feb 28 04:39:20:835 2013 JXSHR-MC-WLAN-AC-H3C-IAG01 RDS/7/DEBUG: Event: Received the detect response from auth-server(IP:211.141.86.107).
*Feb 28 04:39:20:836 2013 JXSHR-MC-WLAN-AC-H3C-IAG01 RDS/7/DEBUG:
Error: The vector of normal-res-packet is invalid(AAAID = 5430, Req-ID = 0).
```

(12) 收集 debug 信息、详细配置信息

如果上述步骤仍无法最终解决问题,可以抓取设备侧详细的 debug 信息辅助定位。注意:开启 debug 之前,请检查 CPU 和内存的使用情况,确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

命令:

```
<AC> debugging portal packet interface xxx
<AC> debugging portal tcp-cheat
<AC> debugging portal acl interface xxx
<AC> debugging radius packet
```

具体 debug 分析参考如下。

第 1 步,http 重定向。

```
*Apr 18 15:01:41:701 2014 AC TCPCHEAT/7/TCPCHEAT_DEBUG: State of connection with source IP 192.168.10.2 is   ESTABLISHED!          //tcp 欺骗,http 重定向
```

第 2 步,Portal 交互。

```
*Apr 27 13:54:57:370 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:16
  Portal check packet OK
Portal packet head:
```

```
Type:1  SN:27   ReqId:0     AttrNum:0  ErrCode:0  UserIP:10.197.58.100
  Portal packet attribute list:
   NULL
  Portal raw packet:
   01 01 00 00 00 1b 00 00 0a c5 3a 64 00 00 00 00       //Portal REQ_CHALLENGE

* Apr 27 13:54:57:370 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal send packet length:34
Portal packet head:
Type:2  SN:27   ReqId:37438 AttrNum:1  ErrCode:0  UserIP:10.197.58.100
  Portal packet attribute list:
   [  3 Challenge          ] [ 18] [a786bd4f07f6e3725ec7880e094c716e]
  Portal raw packet:
   01 02 00 00 00 1b 92 3e 0a c5 3a 64 00 00 00 01
   03 12 a7 86 bd 4f 07 f6 e3 72 5e c7 88 0e 09 4c
   71 6e                                                 //Portal ACK_CHALLENGE

* Apr 27 13:54:57:372 2013 SDJN-WLAN-AC26-HSWX6108-AC1 PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:64
  Portal check packet OK
Portal packet head:
Type:3  SN:27   ReqId:37438 AttrNum:2  ErrCode:0  UserIP:10.197.58.100
  Portal packet attribute list:
   [  1 UserName           ] [ 30] [15194159123@wlan-moni-jituan]
   [  4 ChapPassWord       ] [ 18] [b28071c504a0ad64ffc533a69a8887ba]
  Portal raw packet:
   01 03 00 00 00 1b 92 3e 0a c5 3a 64 00 00 00 02
   01 1e 31 35 31 39 34 31 35 39 31 32 33 40 77 6c       //Portal REQ_AUTH
   61 6e 2d 6d 6f 6e 69 2d 6a 69 74 75 61 6e 04 12
   b2 80 71 c5 04 a0 ad 64 ff c5 33 a6 9a 88 87 ba
```

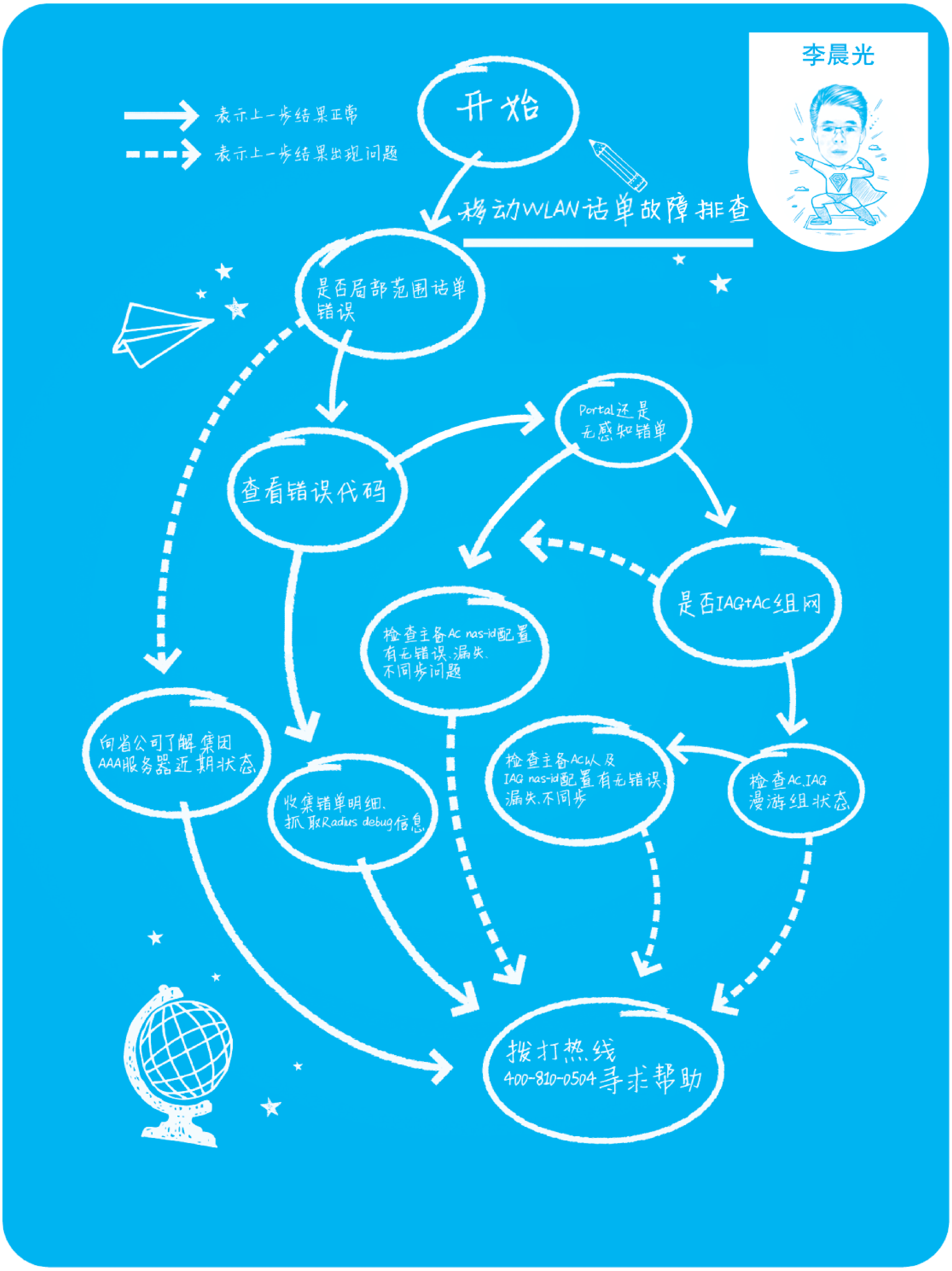
第 3 步，Radius 交互。

```
* Apr 27 13:54:57:380 2013 SDJN-WLAN-AC26-HSWX6108-AC1 RDS/7/DEBUG: Send: IP=
[211.137.185.105], UserIndex=[3108], ID=[175], RetryTimes=[0],Code=[1], Length=[260]
                                        //Radius 认证请求

* Apr 27 13:54:57:396 2013 SDJN-WLAN-AC26-HSWX6108-AC1 RDS/7/DEBUG: Receive: IP=
[211.137.185.105],Code=[2],Length=[106]  //Radius 认证成功响应
```

如果第 3 步中收到服务器 Radius Code=[3]响应报文，则代表 AAA 拒绝用户登录，报文详细解码中一般会携带服务器拒绝的原因。

```
* Jul5 11:18:42:276 2012 SDQDA-WLAN-AC51-HSWX6103-AC RDS/7/DEBUG: Receive: IP=
[221.176.1.138],Code=[3],Length=[149]
* Jul  5 11:18:42:276 2012 SDQDA-WLAN-AC51-HSWX6103-AC RDS/7/DEBUG:
[18 Reply-Message] [129] [18; User ( host/ABE-YB. nt-amphenol1. local ) Checking LoginUser
RBillServer, return Illegal Account, Request Deny by chinamobile.com]
//Radius 认证拒绝消息
```


李晨光
表示上一步结果正常
表示上一步结果出现问题
开始
移动WLAN话单故障排查
是否局部范围话单错误
查看错误代码
Portal还是无感知错单
是否IAG+AC组网
检查主备AC nas-id配置有无错误、漏失、不同步问题
向省公司了解集团AAA服务器近期状态
收集错单明细、抓取Radius debug信息
检查主备AC以及IAG nas-id配置有无错误、漏失、不同步
检查AC、IAG漫游组状态
拨打热线 400-810-0504寻求帮助

1. 开始

本流程图针对问题：移动 Portal、无感知业务中 AAA 认证、计费正常，但无法在移动 BOSS 系统生成业务话单，或者生成错误的业务话单。话单错误问题的第一暴露点不是终端和设备侧，而是集团 BOSS 的话单报表。

所以排查问题的思路是：首先查看错单详细报表，确定问题发生的范围，排除集团服务器侧问题(面的问题)；再排查 AC(点的问题)。

2. 流程图相关操作说明

(1) 是否局部范围话单错误

分析省公司提供的话单统计报表，确定问题发生的范围和频次：错单局限于一台 AC 还是多台 AC；是概率性发生，还是必现问题；以及友商 AC 情况如何。

(2) 向省公司了解集团 AAA 服务器近期状态

可以向集团了解 AAA 服务器侧有无升级操作、临时故障等。

(3) 查看错误代码

话单统计报表会列出错误代码，并简述 BOSS 认为话单错误的原因。

典型的报表信息截取如表 7-8 所示。

表 7-8 典型的报表信息截取

ac_address	duration	prov_code	std_err_code	original_file	remarks
120.192.135.78	28815	531	F111	WLAN_RADIUS_20130326.010	E111:The Stop_time20130326182455 is less than start_time:20130326102440
211.141.11.209	14	431	F150	WLAN_RADIUS_20120728.006	E150:Hotspot_ID foramt error:0951.0431.431.00

目前遇到的两种主要错误代码。

F111：计费时长错误。计费时长超过最长预期 8h，即 28800s。

F150：NAS-ID 格式错误。NAS-ID 错误填充为 AC sysname 或者其他不符合规范的格式。

其他错误代码后续会进一步扩充。

(4) 收集错单明细、抓取 Radius debug 信息

① 对于 F111 错单类型，原因为计费时长超限，大于 8h。需要先观察该条错单计费时长到底为多少。比如表 7-8 中错单计费时长为 28815s，超过 AAA 授权时长 28800 仅 15s 时间，这个时间很可能来自网络传输时延、服务器处理时延等。这种类型的 F111 错误问题需要协调服务器侧进行优化处理，设备侧无法解决。AAA 的授权时长可以通过设备侧的 debug Radius 信息予以确证。

命令：*debugging radius packet*

例如：通过搜索“code=[2]”Radius 认证成功报文，可以看到授权上线时长。

```
<H3C> debugging radius packet
…
*Jul  5 11:04:52:490 2012 SDQDA-WLAN-AC51-HSWX6103-AC RDS/7/DEBUG: Receive: IP=
[221.176.1.138], Code=[2], Length=[318]
*Jul  5 11:04:52:490 2012 SDQDA-WLAN-AC51-HSWX6103-AC RDS/7/DEBUG:
[79 EAP-Message                ] [6 ] [03030004]
[MS-16 MS-MPPE-Send-Key        ] [52] [8852758F6B59502D675692...]
[MS-17 MS-MPPE-Recv-Key        ] [52] [88533C64917C88A67699E7...]
[6  Service-Type               ] [6 ] [2]
[7  Framed-Protocol            ] [6 ] [1]
[1  User-name                  ] [13] [13953110669]
*Jul  5 11:04:52:490 2012 SDQDA-WLAN-AC51-HSWX6103-AC RDS/7/DEBUG:
[27 Session-TimeOut            ] [6 ] [28800]
[18 Reply-Message              ] [117] [0;User(362915C0F9D4C92...)]
[80 Message-Autheticator       ] [18] [8C702E984CC8D98340F6B0B227A5FEC5]
```

② 对于其他错单请收集“original file”。这个文件可以直接通过省公司向集团服务器侧索取，对应的具体文件名可以从话单统计报表中查找得到，如表 7-9 所示。

表 7-9　original file 错单

ac_address	duration	prov_code	std_err_code	original_file	remarks
120.192.135.78	28815	531	F111	WLAN_RADIUS_20130326.010	E111:The Stop_time20130326182455 is less than start_time:20130326102440
211.141.11.209	14	431	F150	WLAN_RADIUS_20120728.006	E150:Hotspot_ID foramt error:0951.0431.431.00

(5) Portal 还是无感知错单

确定错单类型是 Portal 业务错单，还是无感知业务错单。

确定错单的业务类型能有效地帮助定位，业务类型可以通过观察错单统计报表中的“ac_address”项，如果是我司 IAG 地址，则一般为 Portal 业务；如果是 AC 的地址，且该局点位 IAG+AC 组网，则为无感知业务。

(6) 是否 IAG+AC 组网

确定客户现网组网模型，是纯 AC 组网，还是 IAG+AC 组网。

目前 H3C 无线设备的 Portal 认证组网有两种：第一种是 AC 配合 IAG 组网，由 IAG 作为 Portal 认证点完成 Portal 认证；第二种是纯 AC 组网，即 AC 自身作为 Portal 认证点完成 Portal 认证。

两种组网下，无感知认证(802.1x)业务的承载设备都是 AC。

(7) 检查主备 AC NAS-ID 配置有无错误、漏失、不同步问题

AC 上能配置 NAS-ID 的位置非常多，如果重复配置，生效规则有先后顺序。

① 对于 Portal 业务。NAS-ID 生效的先后顺序为：AC 射频视图下配置的 NAS-ID→三层接口下指定的 NAS-ID Profile→三层接口下配置的 Portal NAS-ID→全局配置的 Portal NAS-ID→Sysname。

说明：“AC 射频视图下配置的 NAS-ID”“三层接口下配置的 Portal NAS-ID”“全局配置的 Portal NAS-ID”为必配项。

同时,保证主、备 AC 的 NAS-ID 配置同步。

AC 射频视图下配置 NAS-ID。

```
<H3C> display current-configuration
#
wlan ap jzq_bl model WA2612-AGN id 107
 ap-name 电器_VLAN167_107
 priority level 7
 serial-id 210235A0ALC11B000496
 backup-ac ip 192.168.56.2
 radio 1
  service-template 1nas-id 3731071627000460
  service-template 2nas-id 3731071627000460
  radio enable
#
```

三层接口下配置的 Portal NAS-ID。

```
<H3C> display current-configuration
#
interface Vlan-interface1802
 description GateWay_of_CMCC-EDU
 ip address 10.104.96.2 255.255.224.0
 vrrp vrid 3 virtual-ip 10.104.96.1
 vrrp vrid 3 priority 110
 vrrp vrid 3 track 1 reduced 20
 portal server cmcc-edu method direct
 portal nas-id 3731071627000460
 portal nas-port-type wireless
 portal backup-group 2
 portal nas-ip 218.200.72.36
 access-user detect type arp retransmit 5 interval 10
#
```

全局配置的 Portal NAS-ID。

```
<H3C> display current-configuration
#
portalnas-id 3731071627000460
#
```

② 对于无感知业务。NAS-ID 生效的先后顺序为:AC 射频视图下配置的 NAS-ID→ESS 接口下配置的端口安全 NAS-ID Profile→全局配置的端口安全 NAS-ID Profile→Sysname。

说明:"AC 射频视图下配置的 NAS-ID"为首选方式,其他方式在特定场景下使用,不做强制配置要求。

同时,保证主、备 AC 的 NAS-ID 配置同步。

```
<H3C> display current-configuration
#
wlan ap jzq_bl model WA2612-AGN id 107
 ap-name 电器_VLAN167_107
```

```
 priority level 7
 serial-id 210235A0ALC11B000496
 backup-ac ip 192.168.56.2
 radio 1
  service-template 1nas-id 3731071627000460
  service-template 2nas-id 3731071627000460
  radio enable
#
```

(8) 检查 AC、IAG 漫游组状态

查看 AC 和 IAG 的漫游组状态是否生效。

命令：*display wlan mobility-group*

例如：通过命令查看，AC 是否已经跟 IAG 建立漫游隧道。

```
<AC>display wlan mobility-group
                              Mobility Group Information
--------------------------------------------------------------------
 Group Name              : 1
 Source IP Address       : 218.204.128.155
 Authentication Method   : -NA-
--------------------------------------------------------------------
                                Member Information
--------------------------------------------------------------------
 IP-address        State                      Interface
--------------------------------------------------------------------
 218.204.128.152Run                           WLAN-Tunnel0
--------------------------------------------------------------------
```

(9) 检查主备 AC 以及 IAG NAS-ID 配置有无错误、漏失、不同步

对于 IAG＋AC 组网，在漫游组成功建立的前提下，Portal NAS-ID 优先以 AC 射频视图下的配置生效。具体为如下。

AC 射频视图下配置的 NAS-ID→IAG 三层接口下指定的 NAS-ID Profile→IAG 三层接口下配置的 Portal NAS-ID→IAG 全局配置的 Portal NAS-ID→系统 sysname。

说明：“AC 射频视图下配置的 NAS-ID”、“IAG 全局配置的 Portal NAS-ID”为必配项，后一个配置起保险作用。

同时，保证主备 AC、主备 IAG 的 NAS-ID 配置同步。

AC 射频视图下配置 NAS-ID。

```
<AC> display current-configuration
#
wlan ap jzq_bl model WA2612-AGN id 107
 ap-name 电器_VLAN167_107
 priority level 7
 serial-id 210235A0ALC11B000496
 backup-ac ip 192.168.56.2
 radio 1
  service-template 1nas-id 3731071627000460
  service-template 2nas-id 3731071627000460
```

```
    radio enable
  #
```

IAG 全局配置 Portal NAS-ID。

```
  <IAG> display current-configuration
  #
  portalnas-id 3731071627000460
  #
```



无线PSK认证故障排查
余 晨
表示上一步结果正常
表示上一步结果出现问题
开始
连接SSID是否弹出密码输入框
密钥是否一致
检查WIDS黑白名单配置
检查PSK配置
重置密钥
收集log、trap及debugging信息
拨打热线 400-810-0504 寻求帮助

07 无线产品 > 7.4 认证 > 7.4.6 无线 PSK 认证故障排查 > 步骤详解

1. 开始

PSK(Pre-Shared Key,预共享密钥)认证需要在无线客户端和设备端配置相同的预共享密钥,如果密钥相同,PSK 接入认证成功;如果密钥不同,PSK 接入认证失败。

2. 流程图相关操作说明

(1) 连接 SSID 是否弹出密码输入框

若正确配置了 PSK 认证,终端连接 SSID 会弹出密码输入框,图 7-45、图 7-46 所示分别为 Windows 7 和 iOS 的终端密钥输入页面。

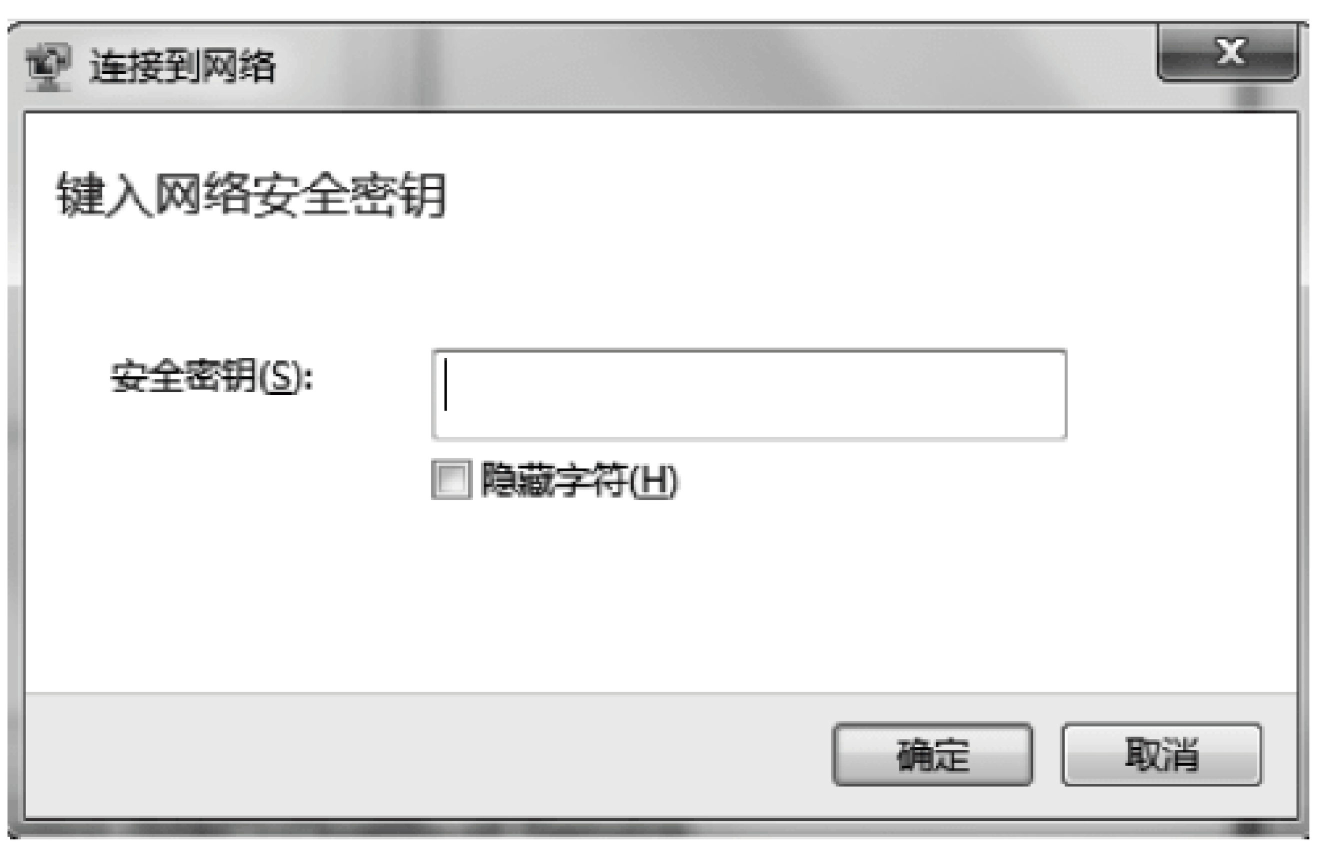


图 7-45　Windows 7 的终端密钥输入页面



图 7-46　iOS 的终端密钥输入页面

(2) 检查 PSK 配置

检查全局端口安全是否开启,终端关联 SSID 对应 ESS 接口的 PSK 配置:端口安全模式为 PSK、使能 11key 类型的密钥协商功能并设置密钥。

```
[AC]display current-configuration
#
port-security enable                    //全局使能端口安全
#
wlan service-template 1 crypto          //服务模板下 SSID 与 ESS 接口对应
ssid 123
 bind WLAN-ESS 1
 cipher-suite tkip
 security-ie rsn
 service-template enable
#
#
```

```
interface WLAN-ESS1
 port access vlan 2
 port-security port-mode psk        //使能端口安全模式为 PSK
 port-security tx-key-type 11key    //使能 11key 类型的密钥协商功能
 port-security preshared-key pass-phrase cipher $c$3$SHcJ950t8GUuMW7zb96l75T9lwDNjtFzbJ43
  //设置密钥
#
```

（3）测试明文关联

创建一个非业务 VLAN 的明文测试 SSID，检查明文关联是否有问题，可参考《无线终端关联失败故障排查云图》。

（4）密钥是否一致

PSK 接入用户必须使用设备上预先配置的静态密钥，即 PSK 与设备进行协商，协商成功后可访问端口；终端在密钥输入页面输入密钥后，若提示密钥不正确，则无法接入无线服务，如图 7-47、图 7-48 所示分别为 Windows 7 和 iOS 的终端密钥错误显示。



图 7-47　Windows 7 的终端密钥错误显示



图 7-48　iOS 的终端密钥错误显示

（5）重置密钥

重新配置预共享密钥。

```
[AC-WLAN-ESS2]port-security preshared-key ?
  pass-phrase   Specify port preshare phrase key     //以字符串方式设置预共享密钥
  raw-key       Specify port preshare raw key        //以十六进制方式设置预共享密钥
[AC-WLAN-ESS2]port-security preshared-key pass-phrase 12345678
```

cipher：以密文方式设置密钥。

simple：以明文方式设置密钥。

以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。设置的明文密

钥或密文密钥，区分大小写。明文密钥为 8～63 个字符的字符串或者长度为 64 位的合法十六进制数；密文密钥为 8～117 个字符的字符串。不指定 cipher 或 simple 时，表示以明文方式设置共享密钥。

（6）收集 diag、debugging 信息

收集 AC 诊断信息和 debugging 信息。

说明：开启 debug 之前，请检查 CPU 和内存的使用情况，确保开启 debug 不会影响设备的正常运行。收集完信息后请及时关闭 debug。

① 当 AC 在线用户数少于或等于 3000 时，建议用下面的命令收集信息并使用调试开关进行调试，尽量避免 console 口和无线登录 AC，信息可能会打印不全，优选有线 telnet。

命令：*debugging wlan mac all*

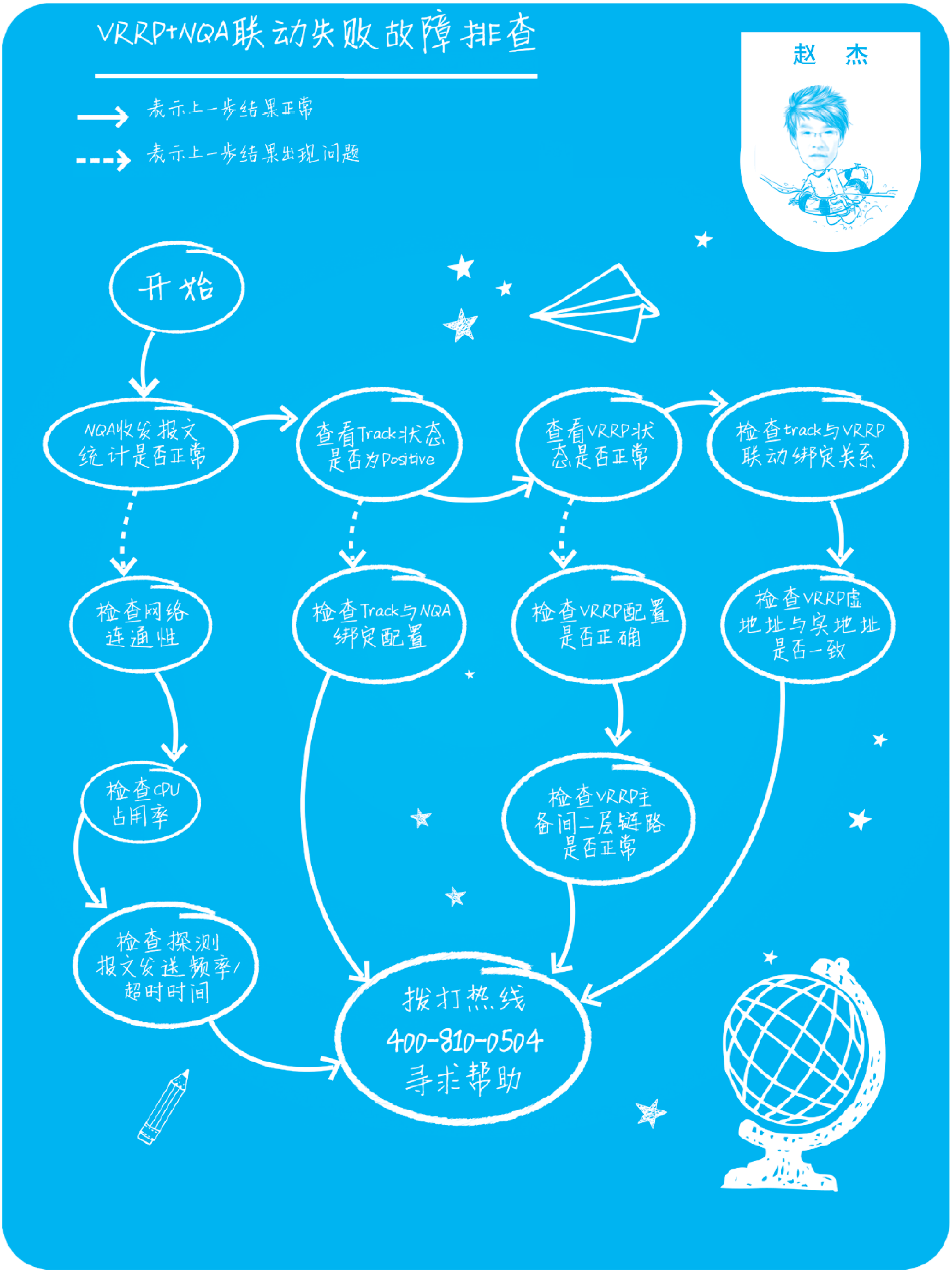
debugging port-security all

debugging dot1xall

terminal monitor

terminal debugging

② 当 AC 在线用户数超过 3000 时，建议等业务闲时关联用户数下降到 3000 以下，再执行上述操作，收集完信息后请关闭 debug。


VRRP+NQA联动失败故障排查
赵 杰
表示上一步结果正常
表示上一步结果出现问题
开始
NQA收发报文统计是否正常
查看Track状态是否为Positive
查看VRRP状态是否正常
检查track与VRRP联动绑定关系
检查网络连通性
检查Track与NQA绑定配置
检查VRRP配置是否正确
检查VRRP虚地址与实地址是否一致
检查CPU占用率
检查VRRP主备间二层链路是否正常
检查探测报文发送频率/超时时间
拨打热线
400-810-0504
寻求帮助

1. 开始

定位故障的思路是：首先观察 NQA 收发统计报文是否一致，判断 NQA 检测是否正常；如果 NQA 检测报文收发不一致且差值数量在增长，则检查网络质量、设备 CPU 利用率以及探测报文发送频率/超时时间的设置；如果 NQA 检查报文收发一致或者收发差值没有增长，则需要检查 Track 状态，如果 Track 状态异常，则需要检查 NQA 配置；如果 Track 状态正常，这需要检查 VRRP 状态是否正常；如果 VRRP 状态异常则需要检查主备之间二层链路是否稳定以及 VRRP 配置是否一致；如果 VRRP 状态正常，则需要检查 Track 与 VRRP 联动配置以及 VRRP 实地址与虚地址是否一致。

2. 流程图相关操作说明

(1) NQA 收发报文统计是否正常

NQA 统计数据记录报文收发数量以及检测失败报文分类统计数量，通过收发报文数量差值可以判断 NQA 检测是否正常，如果多次查看发送报文数量与接收报文数量差值稳定不变，则说明 NQA 探测正常，反之则说明 NQA 探测异常。

命令：*display nqa statistics*

例如：通过命令查看 NQA 报文统计信息，检查发送报文数量和接收数量是否一致，判断 NQA 探测是否正常。

```
[Master]display nqa statistics
  NQA entry (admin admin, tag test) test statistics:
    NO. : 1
  Destination IP address: 192.168.2.10
      Start time: 2015-04-27 13:05:02.2
      Life time: 1351 seconds
      Send operation times:7045              Receive response times: 6620
      Min/Max/Average round trip time: 1/51/5
      Square-Sum of round trip time: 274288
    Extended results:
      Packet loss in test: 6%
      Failures due to timeout:425
      Failures due to disconnect: 0
    Reaction statistics:
      Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
      2        probe-fail        consecutive      7044          425
```

(2) 检查网络连通性

检查 NQA 探测目的地址是否可达，如果目的 IP 地址 ping 不通，主要检查以下内容。

① 检查接口是否 Up，链路是否故障。

② 检查互连端口统计，检查错误报文统计是否在增长。

③ 检查链路状况是否有震荡，是否有端口频繁 Up/Down。

④ 检查 NQA 目的 IP 地址路由是否可达。

⑤ 端口下是否开启了认证、ACL 过滤等安全功能。

⑥ 如果是光介质，检查光衰减是否在正常范围之内。

(3) 检查 CPU 占用率

一般情况下，CPU 利用率超过 90%时可能会导致探测报文上送 CPU 丢包，这时需要排查 CPU 高的原因。

命令：*display cpu-usage*

例如：查看设备的 CPU 占用率。

```
<Master>display cpu-usage
Slot 1 CPU usage:
     92% in last 5 seconds
     90% in last 1 minute
     81% in last 5 minutes
```

(4) 检查探测报文发送频率/超时时间

根据网络的流量大小、设备的性能、链路质量状况等因素，合理配置探测报文的发送间隔以及失效时间。修改 NQA 探测报文的发送间隔和允许连续的探测失败次数。

命令：*frequency interval*

reaction item-number checked-element probe-fail threshold-type consecutive consecutive-occurrences action-type trigger-only

例如：配置 NQA 探测报文发送间隔为 1500ms，最多允许连续 5 个报文失效。

```
[Master-nqa-admin-test-icmp-echo]display this
#
 type icmp-echo
  frequency 1500
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
```

(5) 查看 Track 状态是否为 Positive

通过命令查看 Track 项状态，如果 Track 状态稳定在 Positive，则说明 Track 正常，如果 Track 状态为 Negative 或者 Invalid 状态，则说明 Track 状态异常。

命令：*display track track-entry-number*

例如：通过命令查看 Track 1 的当前状态。

```
[Master]display track 1
Track ID: 1
  Status:Positive
  Duration: 0 days 0 hours 14 minutes 11 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Reference object:
    NQA entry: admin test
    Reaction: 1
```

(6) 检查 Track 与 NQA 绑定配置

配置 Track 项时，如果引用了错误的 NQA 测试组，则该 Track 项的状态为 Invalid。

例如：Track 项错误的引用了 NQA 测试组 admin test Reaction 1 导致 Track 项状态为 Invalid。

```
[Master]display track 1
Track ID: 1
```

```
    Status:Invalid
    Duration: 0 days 0 hours 1 minutes 9 seconds
    Notification delay: Positive 0, Negative 0 (in seconds)
    Reference object:
      NQA entry:admin test
      Reaction:1
  [Master]display nqa reaction counters admin test
    NQA entry (admin admin, tag test) reaction counters:
      Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
      2       probe-fail        consecutive      833           73
```

（7）查看 VRRP 状态是否正常

通过命令检查主备 VRRP 状态是否正常，如果主设备 VRRP 状态为 Master，备设备 VRRP 状态为 Backup，则 VRRP 状态正常，反之若为其他状态则 VRRP 状态异常。

命令：*display vrrp interface vlan x*

例如：通过命令查看主备设备 VLAN1 的 VRRP 状态信息。

```
[Master]display vrrp interface vlan 1
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers on interface Vlan-interface1 : 1
 Interface    VRID   State     Running Adver    Auth       Virtual
                               Pri     Timer    Type           IP
 -----------------------------------------------------------------
 Vlan1        1      Master    120     100      None       192.168.1.1

[Backup]display vrrp interface   vlan 1
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers on interface Vlan-interface1 : 1
 Interface    VRID   State     Running Adver    Auth       Virtual
                               Pri     Timer    Type           IP
 -----------------------------------------------------------------
 Vlan1        1      Backup    100     100      None       192.168.1.1
```

（8）检查 VRRP 配置是否正确

主备的 VRRP 配置保持一致时，VRRP 状态才可以正常，VRRP 关键配置包括 VRID、虚 IP 地址、认证方式以及密钥相同，通过命令检查主备配置是否正常。

命令：*display current-configuration*

例如：使用命令查看检查主备的 VRRP 配置是否一致。

```
[Master]display current-configuration
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 priority reduced 30
#
[Backup]display current-configuration
```

```
#
interface Vlan-interface1
 ip address 192.168.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 100
#
```

（9）检查 VRRP 主备间二层链路是否正常

VRRP 协议通过二层报文相互建立连接，当 VRRP 协议报文转发 VLAN 二层不通时，将影响主备之间的 VRRP 状态，如果 VRRP 协议报文转发 VLAN 二层不通，请检查如下几项。

① 检查接口是否 Up，链路是否故障。

② 检查链路状况是否有震荡，是否有端口频繁 Up/Down。

③ 端口下是否开启了认证、ACL 过滤等安全功能。

④ 如果是光介质，检查光衰减是否在正常范围之内。

（10）检查 Track 与 VRRP 联动绑定关系

如果 Track 状态发生变化，则无法与应用模块联动，检查需要关联的 Track 项是否已创建，或与应用模块关联的 Track 项是否正确。

例如：查看配置的 VRRP 是否与 Track 项正确关联。

```
[H3C]display current-configuration interface vlan 1
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 priority reduced 30
#
return
[H3C]display track 1
Track ID:1
   State: Positive
   Duration: 0 days 1 hours 49 minutes 57 seconds
   Notification delay: Positive 0, Negative 0 (in seconds)
   Tracked object:
     NQA entry: admin test
     Reaction: 1
```

（11）检查 VRRP 虚地址与实地址是否一致

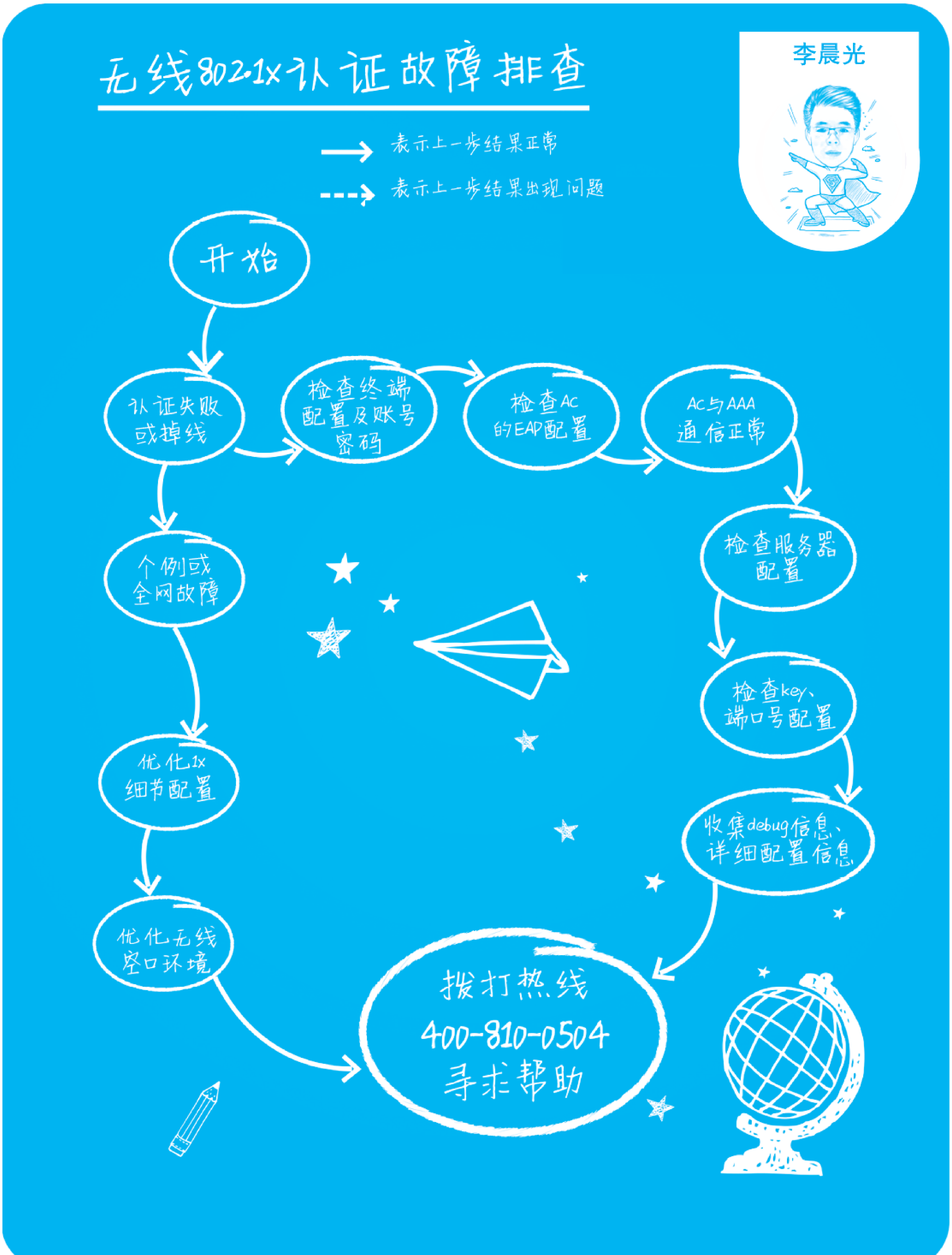
VRRP 正常状态时，设备的 VRRP 虚地址与实地址在同一个网段且不相同，主设备 VRRP 虚地址与实地址相同时，查看主备 VRRP 状态正常，当 NQA 检测到目的地址不可达时，Track 将联动 VRRP 失败，VRRP 状态将不能正常的切换。

命令：*display current-configuration interface vlan x*

例如：使用命令查看 VLAN 接口 VRRP 实地址与虚地址是否相同。

```
[H3C]display current-configuration interface vlan 1
#
interface Vlan-interface1
```

```
ip address192.168.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip192.168.1.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5
 vrrp vrid 1 track 1 priority reduced 30
#
return
```


无线802.1x认证故障排查
李晨光
表示上一步结果正常
表示上一步结果出现问题
开始
认证失败或掉线
检查终端配置及账号密码
检查AC的EAP配置
AC与AAA通信正常
检查服务器配置
检查key、端口号配置
收集debug信息、详细配置信息
个例或全网故障
优化1x细节配置
优化无线空口环境
拨打热线
400-810-0504
寻求帮助

1. 开始

AC 做无线 802.1x 认证,实际是由服务器完成 EAP 方法的定义,如 PEAP、TLS、EAP-SIM。

在 802.1x 认证中,AC 处于通信桥梁的角色,其基本功能是在终端和 AAA 服务器之间建立一条 EAP 报文交互通道。终端和服务器再基于这个通道协商具体的 EAP 认证方法,并完成身份的验证。

定位思路是:先确定问题发生的范围和故障类型,再根据具体情况排查配置细节。另外,设备上的 debug 调试信息是重要的定位手段。

2. 流程图相关操作说明

(1) 认证失败 or 掉线

确定故障类型:是 802.1x 认证失败,用户始终无法访问网络?还是终端能认证成功,且能短暂上网,但是会掉线?可以通过 AC 上命令确定用户能否通过 802.1x 认证。

命令:*display connection access-type dot1x*

例如:通过命令查看 1x 认证用户信息,可以看到用户名和终端 MAC 地址。

```
<AC>display connection access-type dot1x

Index=718 ,Username=luo2@dot1x
MAC=24-77-03-91-77-20
IP=N/A
IPv6=N/A
 Total 1 connection(s) matched.
```

另外,注意识别特殊情况:iphone、ipad、android 等终端在 802.1x 认证成功后,还必须获取 IP 地址,才能显示成功连接 802.11 网络。所以 DHCP 服务器工作异常或者有线网络 VLAN 设置错误也可能导致误判为 802.1x 认证失败。

(2) 个例 or 全网故障

了解掉线问题发生的范围,是全网大多数终端掉线,还是只有个别终端异常。必要时,请尝试更换终端测试,比如 PC、不同型号的手机。

(3) 优化 1x 细节配置

802.1x 认证成功后,默认情况下 AC 设备会开启 1x 握手、重认证等功能,也即是每隔一段时间要求终端重新实施一次 802.1x 认证,这就有可能导致终端发生异常掉线。另外终端在发生无线漫游的时候,会在漫游发生的瞬间出现一个 1x 账号在服务器上有两个用户同时在线的情况,所以需要服务器侧配置允许同一个账号多人登录。

配置优化:关闭 1x 握手、多播触发、1x 重认证等。

```
<H3C>display current-configuration
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 228 298 untagged
 port hybrid pvid vlan 298
```

```
mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 undo dot1x handshake
 undo dot1x multicast-trigger
 undo dot1x re-authenticate
#
```

同时注意 AC 上 Radius Scheme 类型配置。如果出现 1x 掉线的故障，建议先统一修改 Radius Scheme 为 Standard，尝试能否解决。

```
<H3C>display current-configuration
#
radius schemepeap
 server-type standard    //建议统一修改为 Standard 尝试能否解决
 primary authentication10.176.1.138 2645
 primary accounting10.176.1.138 2646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 user-name-format keep-original
 nas-ip 218.200.72.36
 retry stop-accounting 10
#
```

（4）优化无线空口环境

当无线空口环境较差，比如存在 WLAN 外部干扰、信道功率缺乏合理规划、低速率帧占用、无效广播组播报文等，都可能影响 WLAN 通信质量，进而导致 802.1x 掉线。

建议按照《技基通知 2014(005)号—关于下发行业无线优化操作规范的通知》完成网络优化。

（5）检查终端配置及账号密码

如果为 PEAP 方式，检查终端配置、账号密码；如果为 TLS 方式，检查终端证书配置。

例如：PEAP 方式下 Windows XP 客户端配置，如图 7-49 所示。



图 7-49　Windows XP 客户端配置

例如：TLS 方式下个人证书检查，如图 7-50 所示。



图 7-50　TLS 方式下个人证书检查

（6）检查 AC 的 EAP 配置

AC 的 dot1x 配置并不复杂，检查关键的 1x 配置。注意使能 MAC-VLAN 保证 VLAN 授权完成，否则也会导致 dot1x 认证最终失败。另外，建议强制指定 802.1x 认证域。

```
<H3C>display current-configuration
#
 port-security enable
#
 dot1x authentication-method eap
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 228 298 untagged
 port hybrid pvid vlan 298
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 dot1x mandatory-domain peap
 undo dot1x handshake
 undo dot1x multicast-trigger
 undo dot1x re-authenticate
#
```

（7）AC 与 AAA 通信正常

AC 需要与 AAA 直接交互 Radius 协议报文，并使用指定的 IP 地址通信，即 Radius NAS-IP。因此，需要保证 AC 的 RADIUS NAS-IP 与 AAA 服务器路由可达。

测试方法：AC 带源 ping。另外，注意排查网络中的防火墙等设备是否可能阻断 Radius 协议报文。

关于 Radius NAS-IP：AC 可以在 Radius 策略中指定 Radius NAS-IP。

```
<H3C>display current-configuration
#
radius schemepeap
 server-type extended
 primary authentication10.176.1.138 2645
 primary accounting10.176.1.138 2646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 user-name-format keep-original
 nas-ip 218.200.72.36
 retry stop-accounting 10
#
```

（8）检查服务器配置

排查服务器 802.1x 配置，如 EAP 方法的定义、证书，接入设备相关参数定义等。是否配置相同账号允许至少两个用户同时在线等。

（9）检查 key、端口号配置

检查 AC 与 Portal、AAA 通信的 key、端口号配置。服务器侧的配置也需要同步检查。

```
<H3C>display current-configuration
#
radius schemepeap
 server-type extended
 primary authentication10.176.1.138 2645
 primary accounting10.176.1.138 2646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 user-name-format keep-original
 nas-ip 218.200.72.36
 retry stop-accounting 10
#
```

（10）收集 debug 信息、详细配置信息

如果上述步骤仍无法最终解决问题，可以抓取设备侧详细的 debug 信息辅助定位。开启 debug 前检查下 CPU、内存情况，反馈二线确认风险后实施。收集完成后及时关闭。

建议，在业务低峰期抓 debug。业务高峰期可能会有大量其他调试或者日志信息输出，导致有效故障信息打印丢失。

命令：

```
<AC> display radius statistics
<AC> debugging wlan mac event
<AC> debugging wlan mac error
<AC> debugging port-security all
<AC> debugging dot1x all
<AC> debugging sc error
<AC> debugging radius packet
```

08

iMC管理软件


寻尚岩
iMC安装部署故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查部署方式
检查软硬件环境
检查操作系统
检查数据库配置
检查是否专机专用
检查本地文件及版本依赖
检查各进程运行情况及端口占用情况
收集故障现象及相关前后台日志
拨打热线400-810-0504寻求帮助

1. 开始

实际应用中良好的安装和部署 iMC 可以保证网管在安装完成后的正常使用和方便维护。在安装部署过程中，应遵循先做好规划，确认软硬件环境，再安装平台和组件。当出现部署问题时，应根据流程图按照以下步骤依次进行检查。

2. 流程图相关操作说明

(1) 确认部署方式

首先，应根据局点具体需求和所需安装组件来确定部署方式，应参考《智能管理中心(iMC)部署和硬件配置方案》，并根据局点具体业务选择集中式或分布式部署。例如：若在平台和 NTA 组件同时使用，而监控流量较大时，建议选择分布式的部署方式，即平台和 NTA 分别部署在不同的服务器上。另需确认是否需要使用探针服务器。

(2) 检查硬件环境

这一步骤中，如果发现局点部署方式不符合《智能管理中心(iMC)部署和硬件配置方案》对服务器的要求，则需对环境进行整改。

(3) 检查操作系统

根据《智能管理中心(iMC)部署和硬件配置方案》和相应版本平台的版本说明书检查操作系统是否符合要求，相关补丁是否已安装。例如：根据《iMC PLAT 5.2 (E0401) 版本说明书》中要求，当使用 Windows Server 2003 R2 with Service Pack 2(64bit)时，需安装系统补丁 KB942288，如果操作系统不符合要求或补丁未打，则可能在安装后导致进程无法启动等问题。

(4) 检查数据库配置

数据库安装完成后，需要根据相应数据库的安装配置指导书进行配置，这些数据库的配置指导书均可以在安装光盘的/manual 文件夹下找到。如果是 SQL Server 数据库，需配置 TCP/IP 属性，将 SQL Server 置于以“本地系统”的方式启动，并重启 SQL Server 服务。如果是 Oracle 数据库，应为其配置网络服务名、增加监听器的数据库服务并根据实际需求调整 Oracle 的进程数和连接数。Oracle 连接数默认情况下允许 150 个。完成以上配置后，需设置 Oracle 自启动。

(5) 检查是否专机专用

iMC 软件要求专机专用，不可和其他网管类软件或大型软件安装在同一服务器，以免出现软件冲突或产生性能瓶颈。

如有其他杀毒软件外的应用软件，建议删除。

(6) 检查本地文件及版本依赖

注意： 安装包务必拷贝到本地执行安装，请勿远程执行安装。

在该步骤中，应检查本地的安装文件是否正常解压缩。同时，应根据平台和组件的版本说明书，确定版本依赖关系。

(7) 检查各进程运行情况及端口占用情况

iMC 的平台和组件是以固有的 TCP/UDP 端口对外提供服务和访问，如果端口被其他程

序占用则必将导致进程不正常。在 iMC 平台安装和运行后，检查各进程是否是正常运行的，如果有非正常进程，应检查该占用所使用的端口是否被其他程序占用。

检查办法如下。

首先，查看哪个进程启动有异常现象，并在文档《iMC 运行中使用的端口》中找到该进程对应的端口。例如：unbaserver.exe 使用 8052，9099 作为其内部端口。

然后，在该进程所在的服务器上查看该端口是否被占用。以 Windows 系统为例，在“开始”菜单中，找到“运行”，输入“cmd”并按回车键，进入 cmd 命令行，如图 8-1 所示。

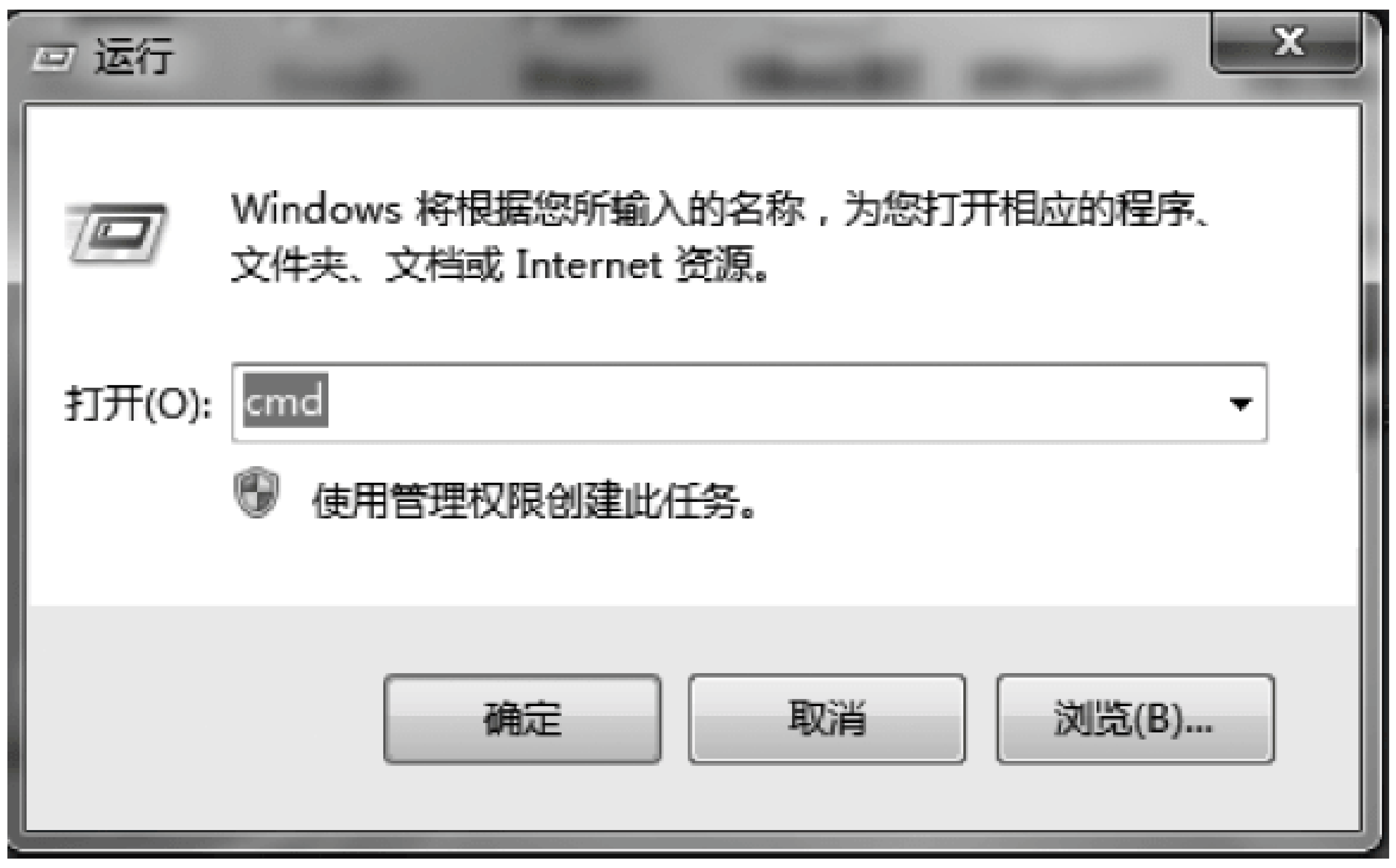


图 8-1 cmd 命令行

在命令提示符下输入命令 netstat -ano | findstr “要查找的端口号”，如要查看使用端口 139 的进程命令和回显，如图 8-2 所示。

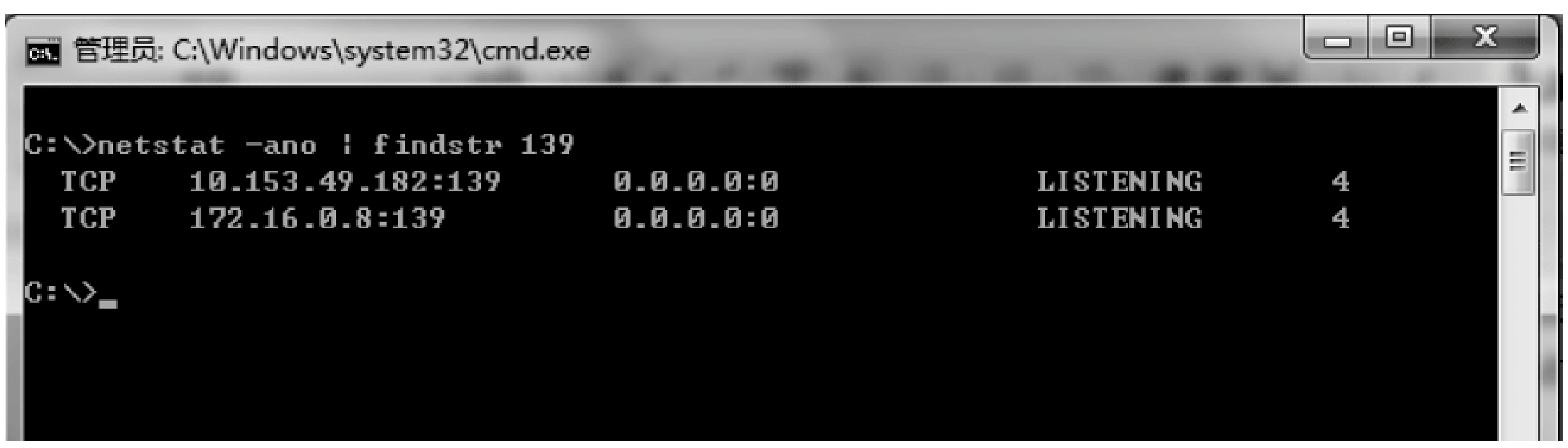


图 8-2 端口 139 的进程命令和回显

由以上可了解使用 139 端口的进程的 PID 为 4，下一步就是根据该 PID 找到具体进程名。

按 Ctrl+Alt+Delete 组合键，进入任务管理器，在菜单中单击“查看”→“选择列”命令，选中 PID(进程标识符)复选框，如图 8-3 所示。

之后即可根据前面了解到的 PID 确定使用该端口的进程是什么，如图 8-4 所示。

由以上即可确认是否是其他进程占用了 iMC 需要的端口。根据局点业务，确认具体情况，如果该进程可以关闭，则关闭该占用 iMC 端口的进程并重启 iMC 异常的进程尝试修复问题。

(8) 收集故障现象及相关前后台日志

在遇到现场问题时，应首先自行定位，排除前面所述各步骤可能的问题。如果仍不能解决问题，应详细收集故障现象、版本信息及前后台日志，拨打热线获取技术支援。

收集信息应根据《业务软件网上问题信息反馈模板》进行收集。

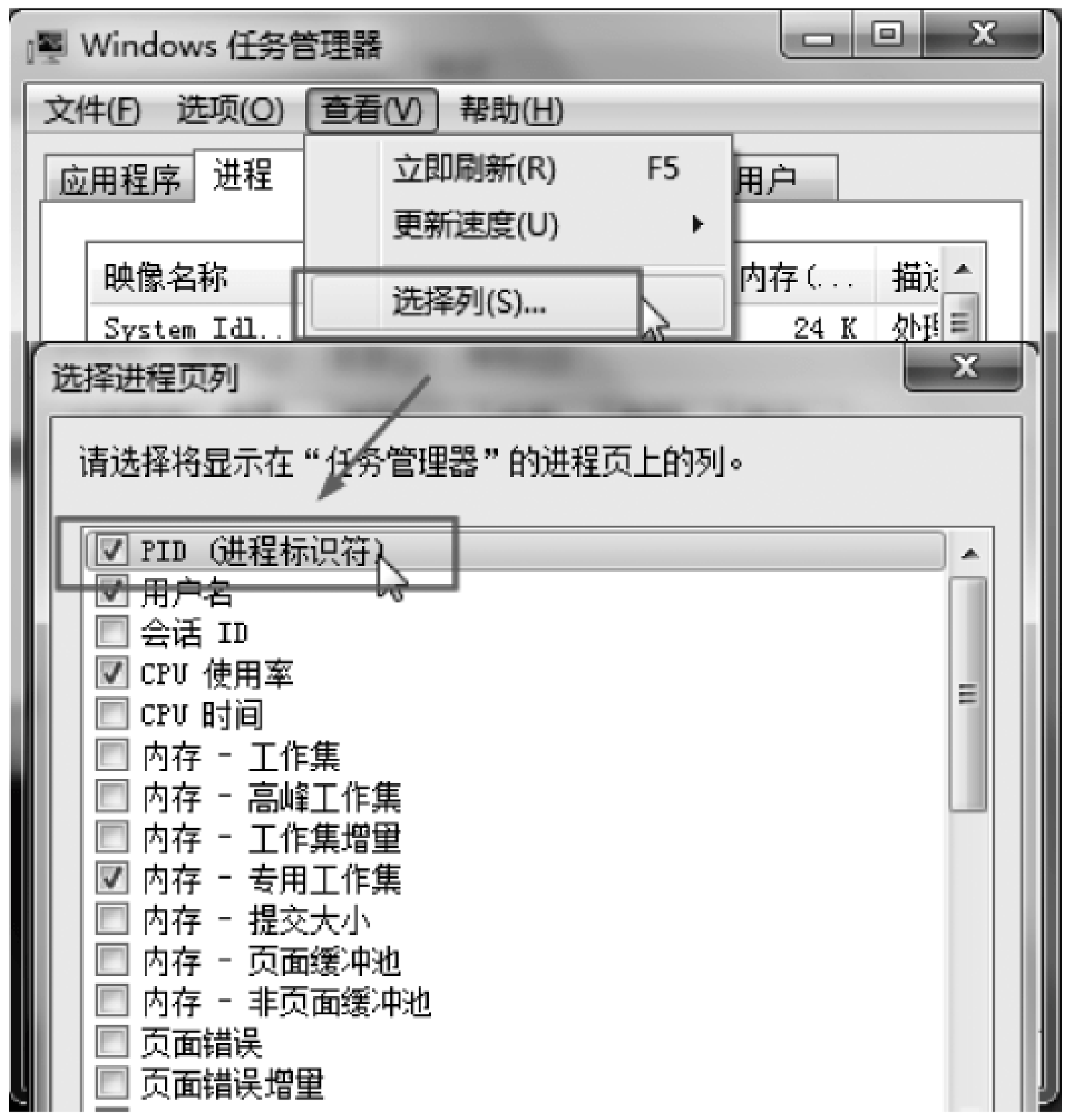
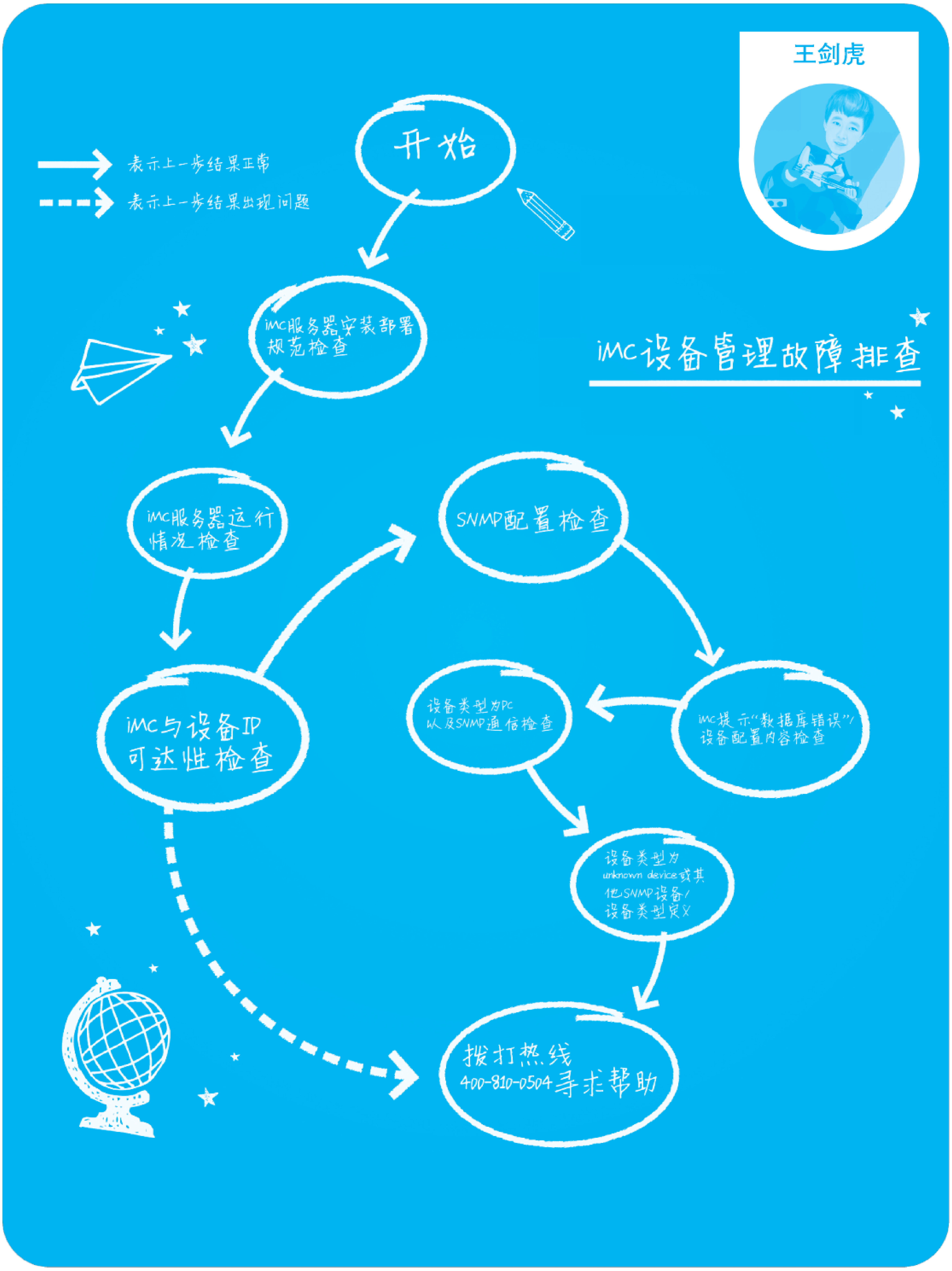


图 8-3　任务管理器



图 8-4　PID 确定使用端口的进程


王剑虎
表示上一步结果正常
表示上一步结果出现问题
开始
iMC设备管理故障排查
iMC服务器安装部署规范检查
iMC服务器运行情况检查
SNMP配置检查
iMC与设备IP可达性检查
设备类型为PC以及SNMP通信检查
iMC提示"数据库错误"/设备配置内容检查
设备类型为unknown device或其他SNMP设备/设备类型定义
拨打热线400-810-0504寻求帮助

1. 开始

管理员在手工增加设备后，就将设备纳入系统的管理，此后用户可以对该设备进行监控及各种操作。本流程故障排查思路主要为 SNMP 配置检查、SNMP 通信超时检查以及设备类型定义检查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

iMC 服务器在网顺利运行的前提之一便是 iMC 服务器的安装部署符合相关规范。该过程主要检查 iMC 服务器的物理性能是否足够承载相关业务，重要组件是否是分布式部署。相关部署要求规范请参考《智能管理中心(iMC)部署和硬件配置方案》。

(2) iMC 服务器运行情况检查

在 iMC 及其组件的部署符合相关规范的前提下，需要对 iMC 服务器的运行情况进行检查。该过程检查服务器的 CPU/内存利用率是否正常、数据库运行是否正常以及 iMC 是否有未启动进程。

(3) iMC 与设备 IP 可达

iMC 能够管理设备的必要条件之一便是 iMC 与设备能够 IP SNMP 可达，建议设备的管理 IP 为环回地址。

(4) SNMP 配置检查

该步骤主要检查 iMC 侧 SNMP 配置与设备侧 SNMP 配置是否一致，在 iMC 侧设备详细信息页面，单击修改 SNMP 参数，即可获知 iMC 侧 SNMP 配置。在设备侧命令行执行[H3C] display current-configuration | include snmp 即可获知当前设备 SNMP 配置。

(5) iMC 提示"数据库错误"/设备配置内容检查

设备添加失败的情况之一为 iMC 显示数据库错误，如图 8-5 所示。

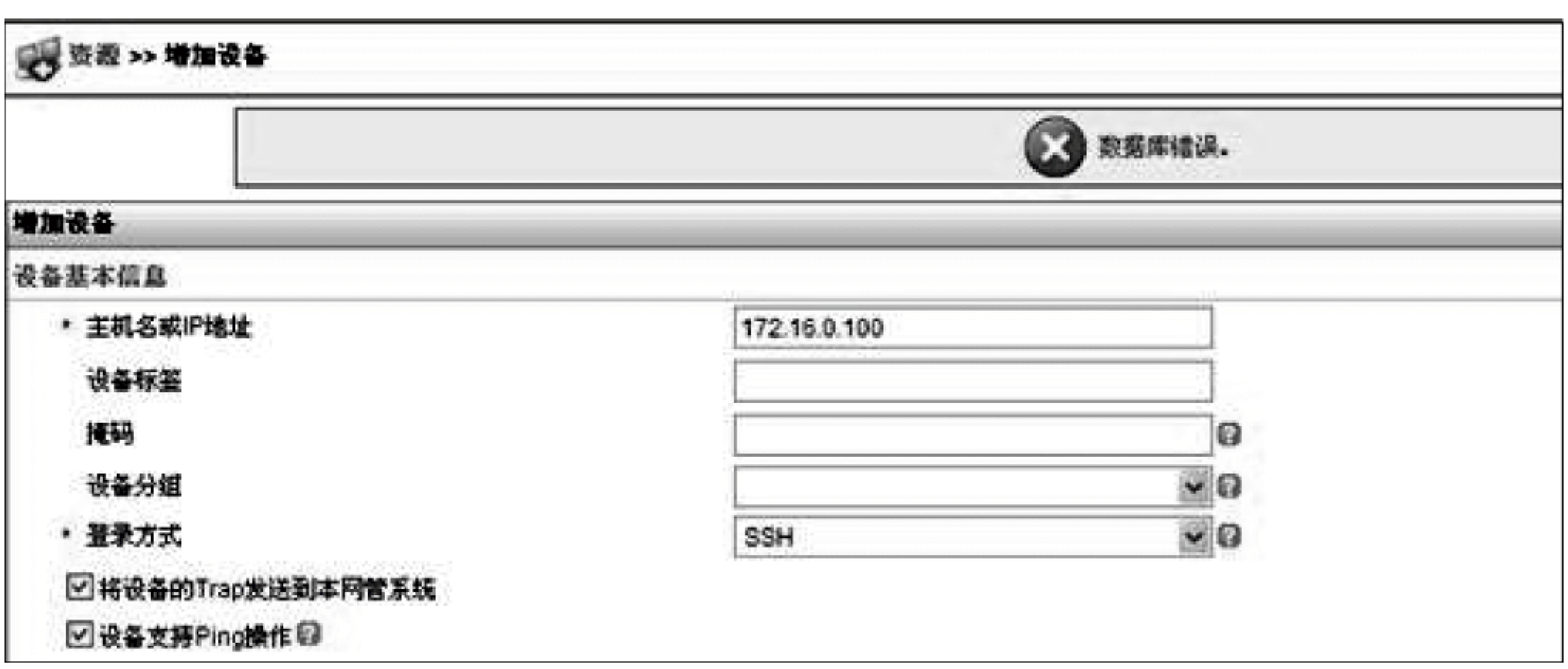


图 8-5 iMC 显示数据库错误

添加设备时显示数据库错误的原因一般为设备配置内容中存在中文字符导致 iMC 将相关信息写入数据库表项中出现错误，建议查看设备配置，将相关配置信息修改为英文。

```
[H3C-GigabitEthernet2/0/16]display this
#
interface GigabitEthernet2/0/16
 port link-mode route
 description 仁中角忍
 ip address 100.0.0.1 255.255.255.0
 mpls
 mpls ldp
#
```

(6) 设备类型为 PC 以及 SNMP 通信检查

设备添加失败的情况之一是设备类型为 PC，见图 8-6。



图 8-6　设备类型为 PC

设备类型识别为 PC 的主要原因是 iMC 与设备 SNMP 通信出现故障。

SNMP 配置主要分为 iMC SNMP 参数配置和设备 SNMP 参数配置，对于二者典型配置方法分别如下。

设备 SNMP 配置如下。

```
<H3C>dis current-configuration | include snmp
 snmp-agent
 snmp-agent local-engineid 800063A203C4CAD9D3F751
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info versionall
 snmp-agent target-host trap address udp-domain 172.16.0.9 params          securityname public
```

iMC SNMP 配置如下。

依次单击“资源”→“增加设备”命令，可在图 8-7 所示界面中配置相关参数。

也可定制 SNMP 模板，从已有的 SNMP 参数模板中选取。

依次单击“系统管理”→“资源管理”→“SNMP 模板”命令，该处可增加、删除 SNMP 模板，系统默认 default 模板，见图 8-8。

一般情况下可通过修改 SNMP 超时以及检查防火墙是否过滤了 SNMP 报文来解决问题。可在设备详细信息页面“配置”选项框中“修改 SNMP 参数”来调高 SNMP 超时，见图 8-9。



图 8-7 SNMP 参数设置界面

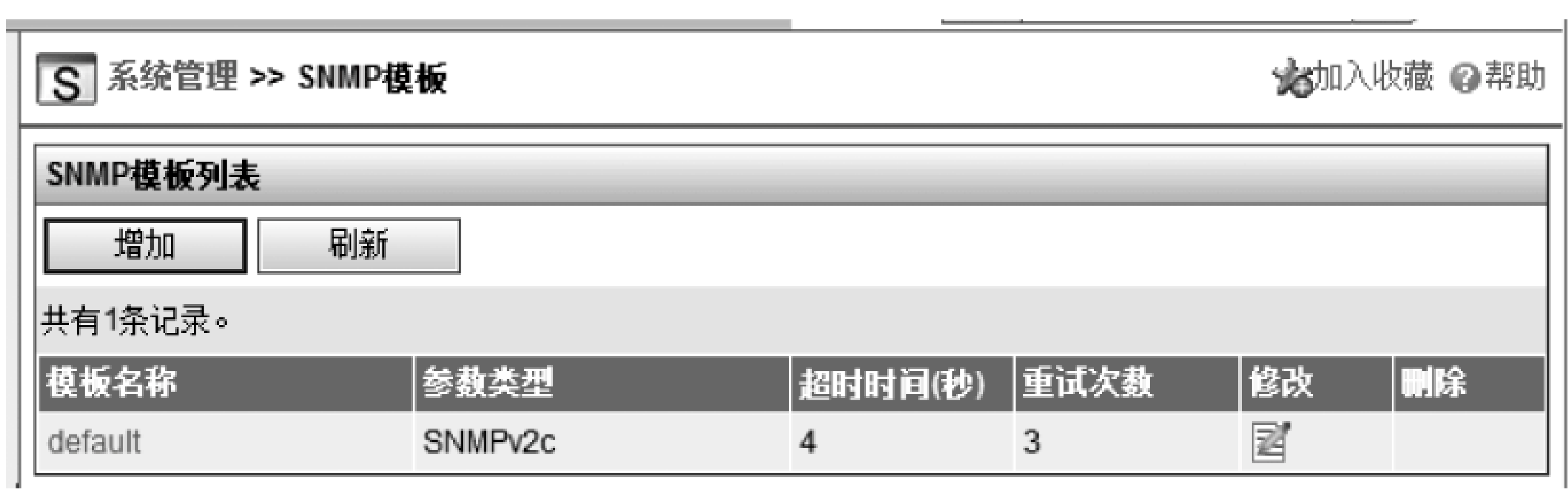


图 8-8 系统默认 default 模板



图 8-9 设备详细信息页面

(7) 设备类型为 unknown device 或其他 SNMP 设备/设备类型定义

设备添加失败的情况之一为设备类型为其他 SNMP 设备。

设备类型被识别为 unknown device 或其他 SNMP 设备的原因一般为设备型号 sysoid 未在 iMC 中与设备型号做预先关联。可通过单击“系统管理”→“资源管理”命令中定义“设备系列”“设备型号”以及“设备类型”来解决,见图 8-10。

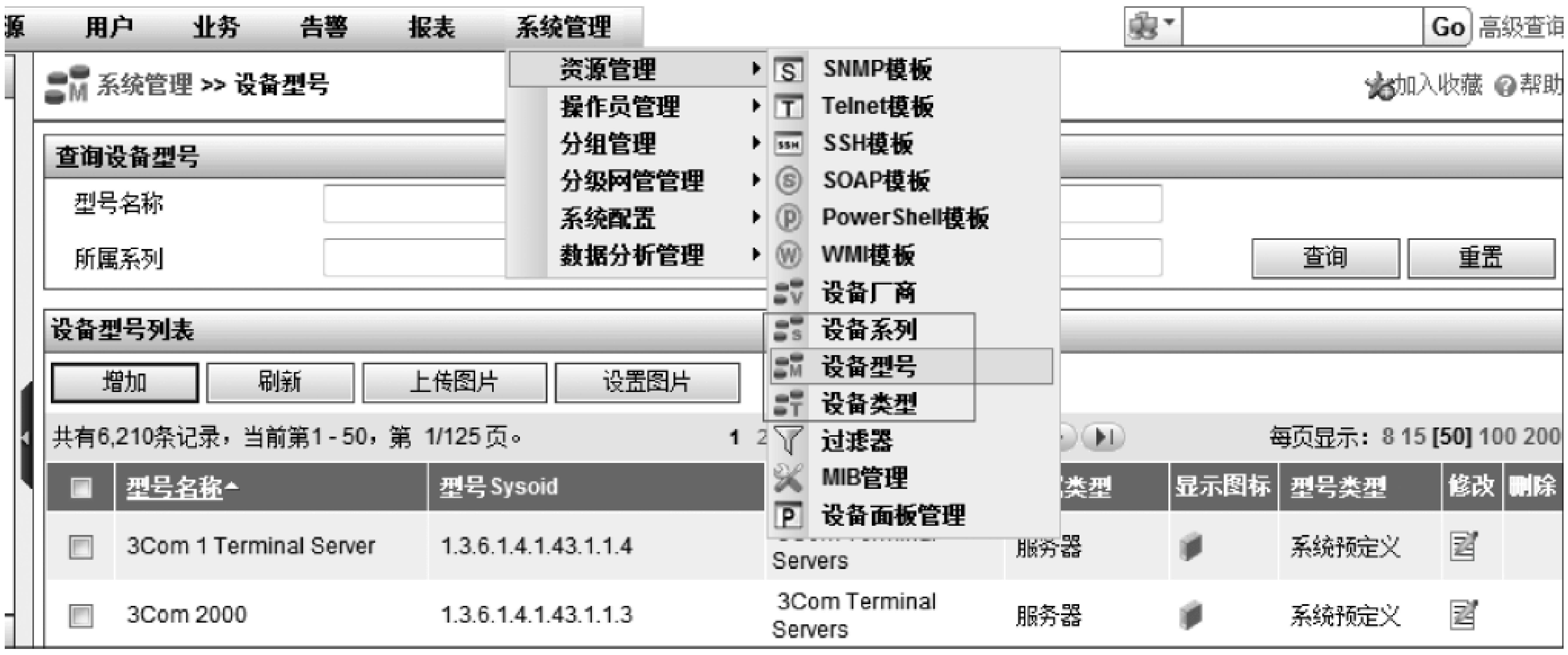
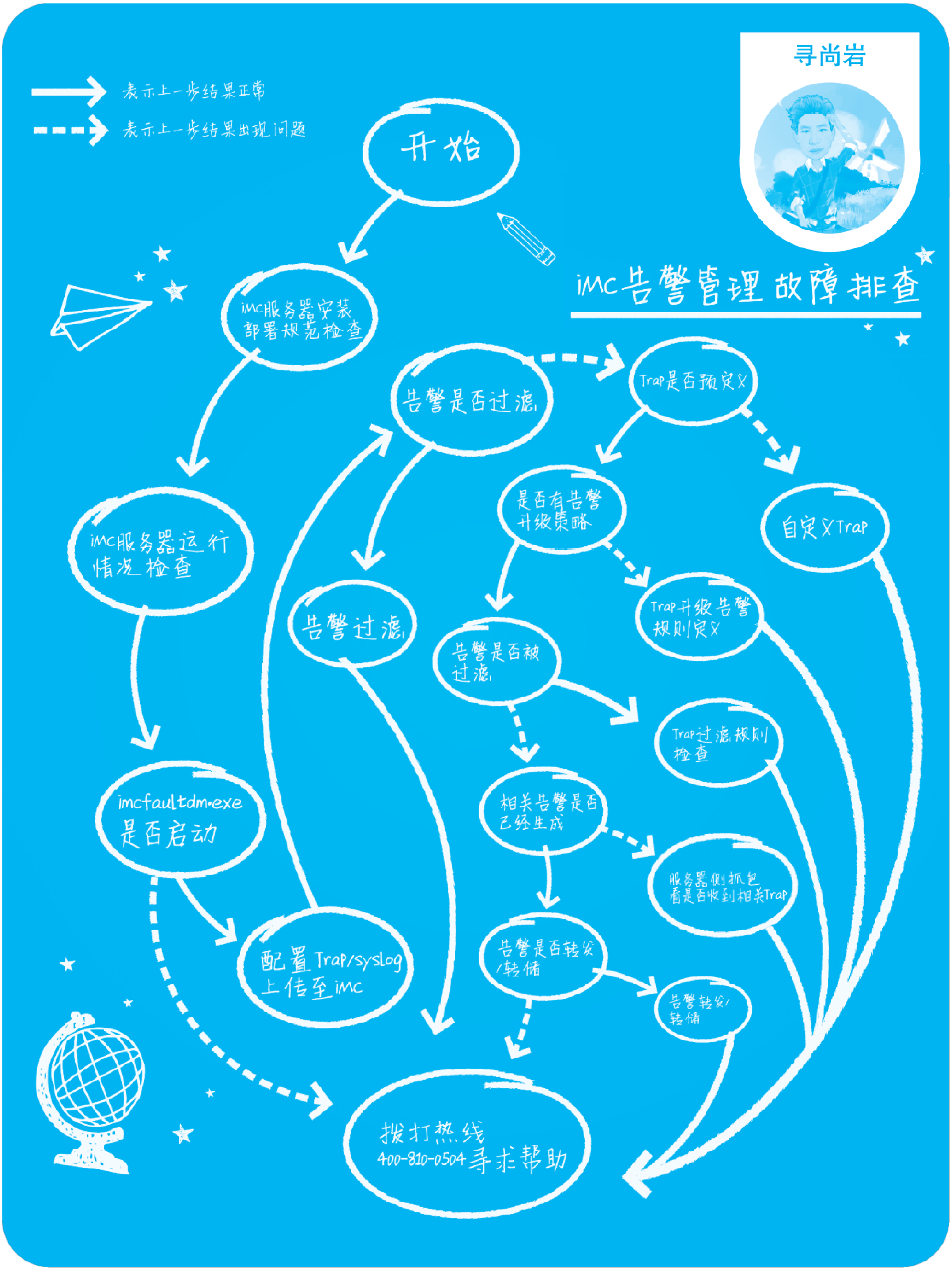

用户
业务
告警
报表
系统管理
Go 高级查询
系统管理 >> 设备型号
加入收藏 帮助
资源管理
操作员管理
分组管理
分级网管管理
系统配置
数据分析管理
SNMP模板
Telnet模板
SSH模板
SOAP模板
PowerShell模板
WMI模板
设备厂商
设备系列
设备型号
设备类型
过滤器
MIB管理
设备面板管理
查询设备型号
型号名称
所属系列
查询
重置
设备型号列表
增加
刷新
上传图片
设置图片
共有6,210条记录，当前第1 - 50，第 1/125 页。
每页显示：8 15 [50] 100 200
型号名称
型号 Sysoid
显示图标
型号类型
修改
删除
3Com 1 Terminal Server
1.3.6.1.4.1.43.1.1.4
Servers
服务器
系统预定义
3Com 2000
1.3.6.1.4.1.43.1.1.3
3Com Terminal Servers
服务器
系统预定义

图 8-10　资源管理


寻尚岩
表示上一步结果正常
表示上一步结果出现问题
iMC告警管理故障排查
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
imcfaultdm.exe是否启动
配置Trap/syslog上传至iMC
告警是否过滤
告警过滤
Trap是否预定义
自定义Trap
是否有告警升级策略
Trap升级告警规则定义
告警是否被过滤
Trap过滤规则检查
相关告警是否已经生成
服务器侧抓包看是否收到相关Trap
告警是否转发/转储
告警转发/转储
拨打热线400-810-0504寻求帮助

1. 开始

iMC 网管特色功能之一是提供了丰富的告警管理功能，该功能包含告警的定义、过滤、syslog 升级告警、转发以及告警转储等特性。本流程排查的主要思路为进程检查、配置检查、告警预定义检查、告警升级策略检查、告警过滤检查以及告警的转储配置。

2. 流程图相关操作说明

（1）iMC 服务器安装部署规范检查

iMC 服务器在网顺利运行的前提之一便是 iMC 服务器的安装部署符合相关规范。该过程主要检查 iMC 服务器的物理性能是否足够承载相关业务，重要组件是否分布式部署。相关部署要求规范请参考《智能管理中心(iMC)部署和硬件配置方案》。

（2）iMC 服务器运行情况检查

在 iMC 及其组件的部署符合相关规范的前提下，需要对 iMC 服务器的运行情况进行检查。该过程检查服务器的 CPU/内存利用率是否正常、数据库运行是否正常以及 iMC 是否有未启动进程。

（3）imcfaultdm.exe 进程是否启动

可在服务器上执行如下命令行。

netstat -aon | findstr 0.0.0.0:162 来判断 Trap 接收端口是否处于侦听状态，如图 8-11 所示。

```
C:\Users\Administrator>netstat -aon | findstr 0.0.0.0:162
  UDP    0.0.0.0:162            *:*                                    6092
```

图 8-11　判断 Trap 接收端口是否处于侦听状态

由图 8-11 可知 162 端口被 PID 为 6092 的进程占用，如图 8-12 所示。

映像名称	. ▲	用户名	CPU	内存(...	描述
tam.exe *32	5756	SYSTEM	00	8,012 K	tam
imcwlandm.exe *32	5760	SYSTEM	00	28,164 K	imcwlandm
sogouexplorer.exe *32	5836	Admin...	00	32,764 K	搜狗高...
uam.exe *32	5872	SYSTEM	00	1,668 K	uam
imcwipsdm.exe *32	5888	SYSTEM	00	10,076 K	imcwipsdm
imcapmedm.exe *32	5896	SYSTEM	00	14,964 K	imcapmedm
imcmplsvpndm.exe *32	5904	SYSTEM	00	13,376 K	imcmpls...
imcmplsdm.exe *32	5916	SYSTEM	00	18,524 K	imcmplsdm
imcmplstpdm.exe *32	5924	SYSTEM	00	19,412 K	imcmpls...
imctedm.exe *32	5932	SYSTEM	00	11,360 K	imctedm
imcl2vpndm.exe *32	5940	SYSTEM	00	10,432 K	imcl2vpndm
dbman.exe *32	5948	SYSTEM	00	1,452 K	dbman
imcnetresdm.exe *32	6060	SYSTEM	00	22,768 K	imcnetr...
imcl2topodm.exe *32	6068	SYSTEM	00	12,924 K	imcl2to...
imcjobmgrdm.exe *32	6076	SYSTEM	00	8,888 K	imcjobm...
imccmdmgrdm.exe *32	6084	SYSTEM	00	8,380 K	imccmdm...
imcfaultdm.exe *32	6092	SYSTEM	00	18,592 K	imcfaultdm
imcupgdm.exe *32	6100	SYSTEM	00	8,556 K	imcupgdm

图 8-12　162 端口被 PID 为 6092 的进程占用

由上图可知 imcfaultdm.exe 的进程 PID 为 6092，为 iMC 进程。若为非 imcfaultdm.exe 进程，则可通过在 DOS 窗口执行 taskkill -f -pid 6092 来终止该进程，在 iMC 部署监控代理中手工启动 imcfaultdm.exe 来保证 iMC 能正确接收到相关 Trap。

说明：一般情况下，kill 进程均为风险操作，操作前须和客户做好沟通。

（4）配置 Trap 上送至 iMC

iMC 产生设备相关告警的前提便是设备及时将 Trap 等信息让送至 iMC。

Trap 上送至 iMC 配置如下。

```
[H3C]snmp-agent target-host trap address udp-domain 172.16.0.9 params
     securityname public
[H3C]info-center enable
[H3C]snmp-agent  trap source LoopBack 0
```

（5）告警过滤/过滤规则配置

iMC 是否生成告警由操作员决定。iMC 默认定义了四条过滤规则，分别为重复 Trap 过滤、闪断 Trap 过滤、未知 Trap 过滤以及未管理设备 Trap 过滤。相关过滤规则描述见图 8-13。



图 8-13　过滤规则描述

iMC 支持操作员在预定义 Trap 过滤规则的基础上自行定义 Trap 规则，该特性支持操作员对 Trap、设备、端口以及时间段进行定义，从各个维度来控制 iMC 告警的生成，见图 8-14。

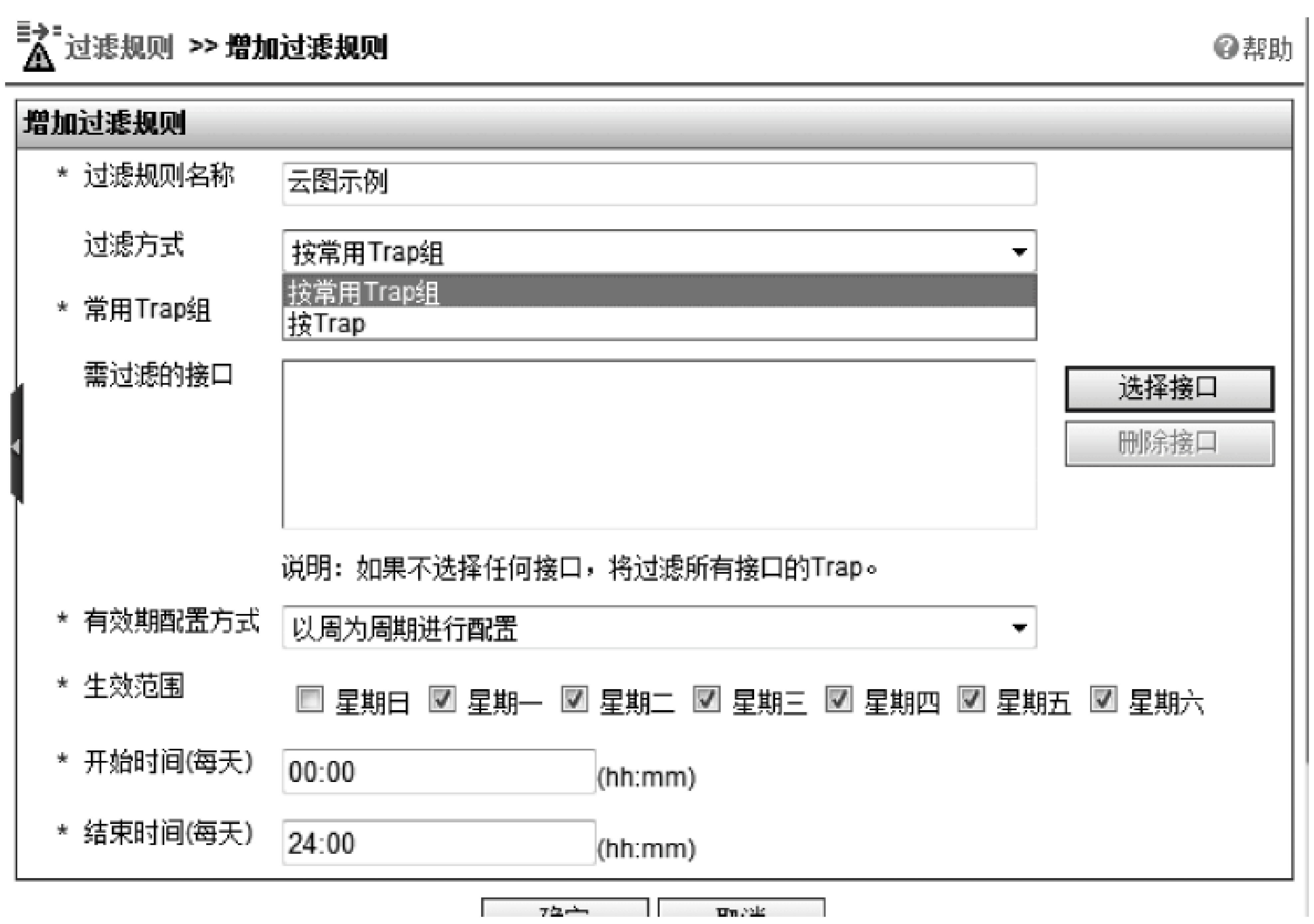


图 8-14　从各维度控制 iMC 告警生成

（6）Trap 是否预定义

iMC 预定义了若干 Trap 来与设备上送的 Trap 进行匹配，若设备上送 Trap 未在 iMC 中

预定义,则 iMC 不能正确解析该 Trap。

依次单击"告警"→"Trap 管理"→"Trap 定义一览表"来查看 iMC 自定义的 Trap。

(7) 自定义 Trap

通过在"Trap 定义一览表"中单击"增加"可自定义一个 Trap,详细界面见图 8-15。



图 8-15　Trap 的详细界面

相关参数说明请详见 iMC 联机帮助。

(8) 是否有告警升级策略/Trap 升级告警规则定义

在步骤(7)的基础上,还需配置 Trap 升级为告警规则。依次单击"告警"→"Trap 管理"→"Trap 升级为告警"→"增加 Trap 升级为告警规则"命令,可查看系统默认的 Trap 升级为告警规则。在该页面中单击"增加"按钮可新建 Trap 升级为告警规则,可从关键字、Trap 源、Trap 类型以及时间等维度来定义一个规则,如图 8-16 所示。



图 8-16　从各维度定义的规则

相关信息请参考 iMC 联机帮助。

(9) 判断告警是否被过滤/Trap 过滤规则检查

在上述步骤以及配置都正确的前提下,iMC 可能未产生相关告警。对于该种场景,需要检查 iMC 现有告警过滤规则是否将相关告警过滤。需要判断设备是否经常生成该 Trap,该 Trap 是否被 iMC 当作重复 Trap 过滤,如图 8-17 所示。



图 8-17 Trap 是否被 iMC 当作重复 Trap 过滤

(10) 告警是否生成以及 iMC 抓包查看是否收到 Trap

在步骤(9)中找到相关的 Trap 过滤项的前提下,iMC 还未生成相关告警,则需要在服务器进行抓包,wireshark 软件筛选条件为 ip. src_host==x. x. x. x and udp. dstport==162。

若未抓取到相关数据包,则需要进行排查网络中是否有防火墙将 Trap 报文过滤等操作。

(11) 告警是否转发

iMC 支持将告警通过邮件、短信、转发至其他网管的方式进行转发。相关转发配置详见步骤告警转发。

(12) 告警转发

邮件转发:分为两个部分,分别为邮件服务器配置和告警通知与转发配置。邮件服务器配置可通过单击“系统管理”→“邮件服务器配置”命令来指定发送告警的邮件地址,如图 8-18 所示。



图 8-18 发送告警的邮件地址

邮件转发配置可通过单击“告警”→“告警设置”→“通知与转发”→“增加邮件通知”命令来指定需要将哪些告警发送至哪个邮箱，如图 8-19 所示。



图 8-19　指定告警发至的邮箱

短信转发：该转发方式需要在 iMC 服务器上配置一短信猫。

转发至其他网管：单击“告警”→“告警设置”→“通知与转发”→“增加告警转发”命令来指定需要将哪些告警发送至哪个 IP，如图 8-20 所示。



图 8-20　指定告警发至的 IP

(13) 告警是否转储

随着告警数据量的增长，可能出现服务器磁盘空间不足的现象。在该情形下可通过告警转储来保留相关数据。相关配置详见步骤告警转储。

(14) 告警转储

依次单击“系统管理”→“数据转储配置”命令来配置告警转储，如图 8-21 所示。

需要说明的是，对于设备告警，只有已恢复告警才会进行转储。若告警未恢复，则当其持续时间超过 30 天会自动变为恢复状态。对于设备 Trap，则该 Trap 是否被恢复都会进行转储。

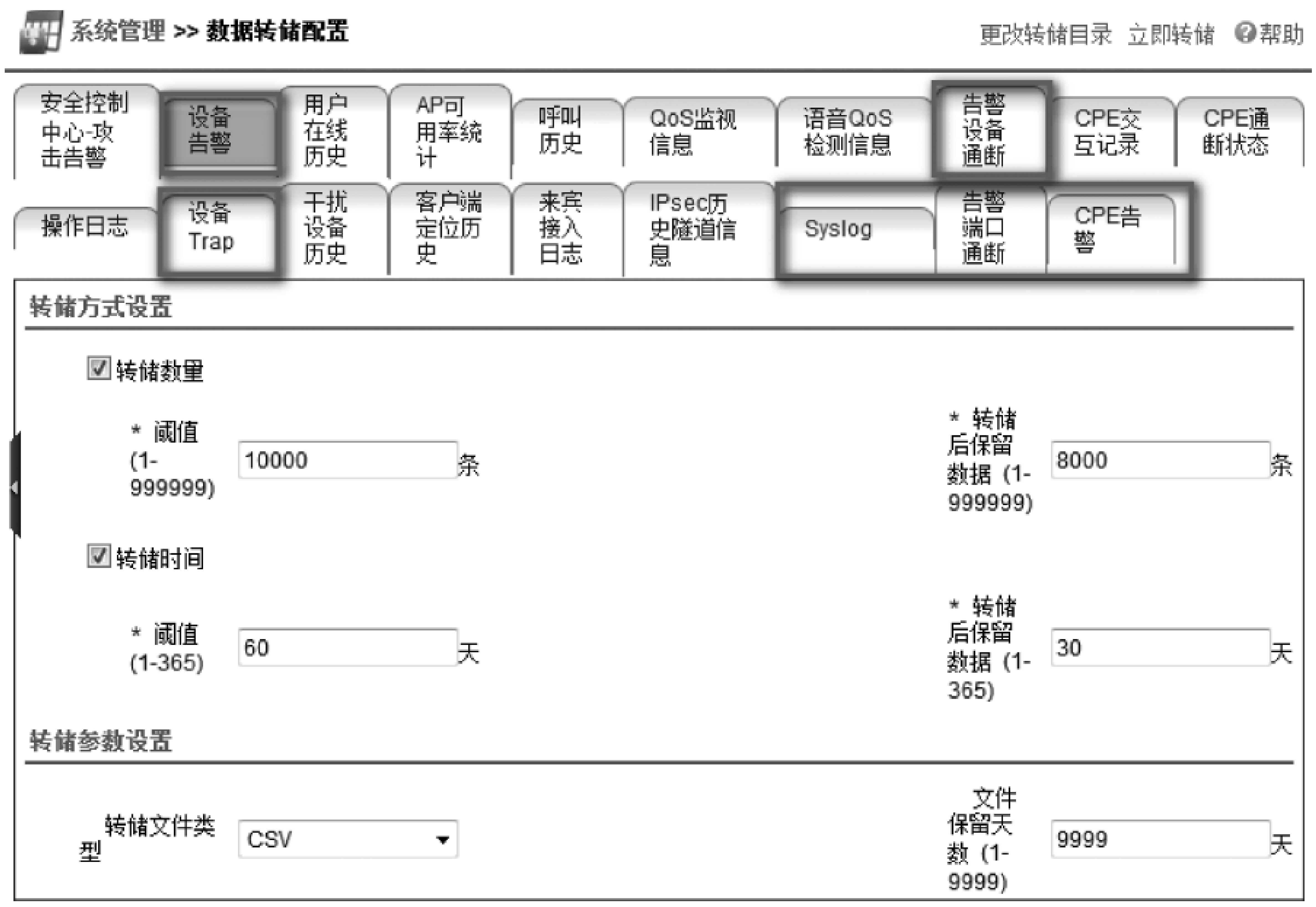
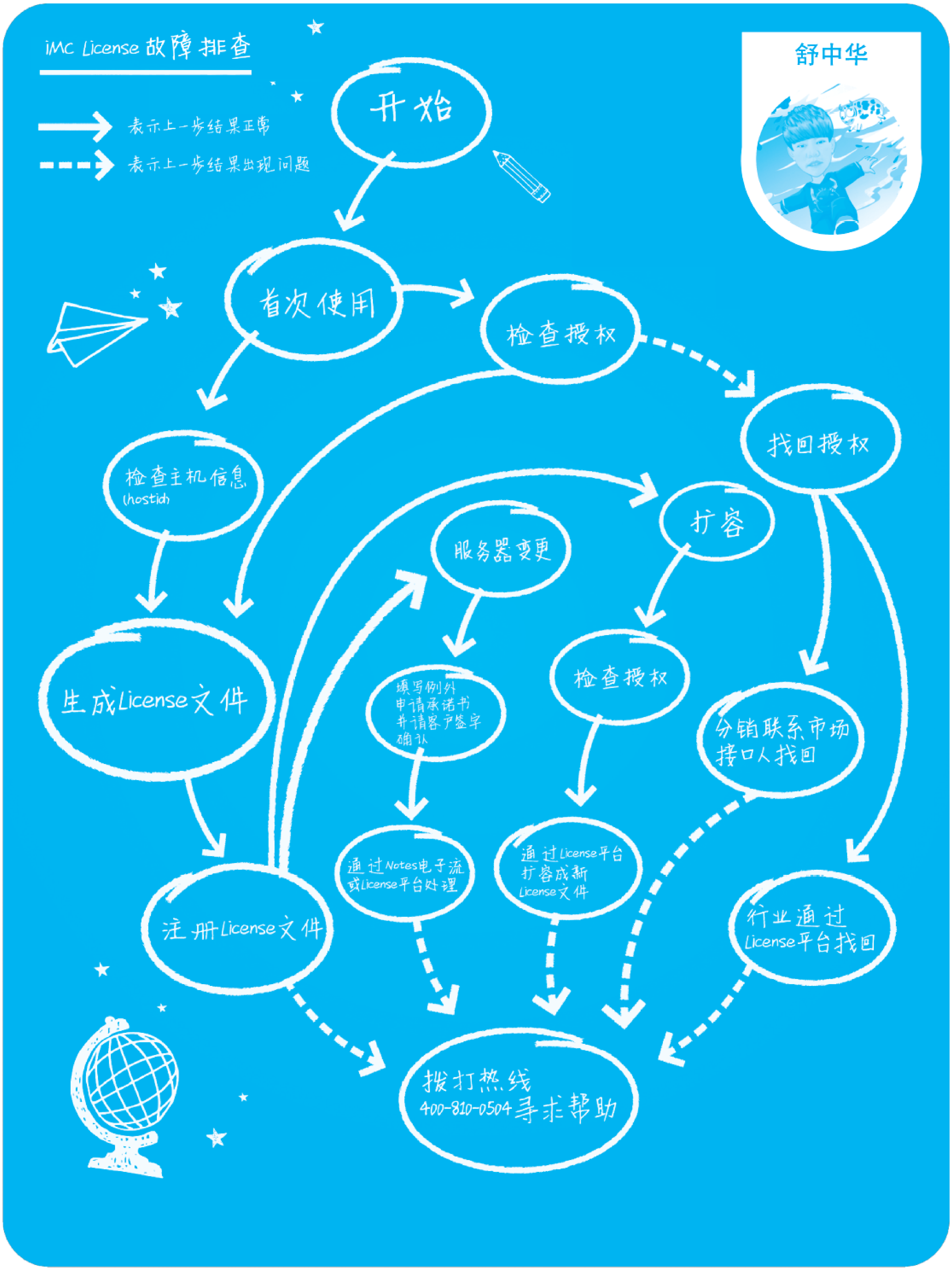

系统管理 >> 数据转储配置
更改转储目录 立即转储 帮助
安全控制中心-攻击告警
设备告警
用户在线历史
AP可用率统计
呼叫历史
QoS监视信息
语音QoS检测信息
告警设备通断
CPE交互记录
CPE通断状态
操作日志
设备Trap
干扰设备历史
客户端定位历史
来宾接入日志
IPsec历史隧道信息
Syslog
告警端口通断
CPE告警
转储方式设置
转储数量
* 阈值 (1-999999)
10000
条
* 转储后保留数据 (1-999999)
8000
条
转储时间
* 阈值 (1-365)
60
天
* 转储后保留数据 (1-365)
30
天
转储参数设置
转储文件类型
CSV
文件保留天数 (1-9999)
9999
天

图 8-21 告警转储配置


iMC License 故障排查
表示上一步结果正常
表示上一步结果出现问题
舒中华
开始
首次使用
检查授权
找回授权
检查主机信息 (hostid)
扩容
服务器变更
生成License文件
检查授权
填写例外
申请承诺书
并请客户签字
确认
分销联系市场
接口人找回
通过Notes电子流
或License平台处理
通过License平台
扩容成新
License文件
注册License文件
行业通过
License平台找回
拨打热线
400-810-0504寻求帮助

1. 开始

iMC 的各项功能的使用依赖于各项授权，所有的授权码和唯一标识服务器硬件信息的 hostid 进行绑定形成 License 文件，在 License 文件导入到 iMC 中并重新启动 iMC 服务，所有授权才会正式生效。

在该流程中，有部分操作是相同或类似的，本文档仅对首次出现的流程进行说明。

2. 流程图相关操作说明

(1) 首次使用

说明：首次使用 License 是针对某一个 iMC 的一套授权来讲的，而不是针对某个工程师第一次使用 License。首次使用即表明授权已确定符合客户需求，不涉及服务器变更或授权扩容等情况。

(2) 检查授权

检查授权是否符合客户需求。如果授权丢失，应通过"找回授权"进行找回。

(3) 检查主机信息(hostid)

主机信息是使用服务器硬件信息来唯一标识服务器的，在收集后会形成名为 hostid 文件。

以下是收集主机信息的方法。

在 iMC 登录页面上单击"产品注册"按钮，如图 8-22 所示。



图 8-22 iMC 登录页面

在新页面中输入 admin 的密码，选择"申请新的 License 或升级现有的 License"，并单击"下一步"按钮，如图 8-23 所示。



图 8-23 选择操作

在下一步中输入相关信息后，单击"确定"按钮即下载该服务器 hostid，该操作在任何可以访问 iMC 的终端上执行均可，不必在 iMC 服务器上操作。

在首次为 iMC 申请 License 和进行扩容时都需要执行收集主机信息的操作。

说明：收集主机信息，原有 License 将在 14 天后失效。仅当需要升级 License 时，才应该执行该操作！

(4) 生成 License 文件

生成 License 文件的过程即把授权信息和主机信息进行绑定的过程。在操作需在 License 平台上进行，首次使用和扩容时都需进行此步骤。

License 平台的地址如下。

lmp. h3c. com（H3C 内网）。

licenseing. h3c. com（公网）。

登录 License 平台，单击“License 激活管理”→“License 首次激活申请”命令，如图 8-24 所示。

根据网页提示上传相关文件并输入客户信息，单击“生成”按钮即可。

在扩容时，单击“License 激活管理”→“License 扩容激活申请”命令，其他操作类似。

说明：在从临时 License 文件扩容为正式 License 文件时，应在扩容时将原有临时授权剔除再添加正式授权，避免因此临时授权过期导致整个 License 失效。

(5) 注册 License 文件

在 iMC 登录页面上单击“产品注册”按钮，如图 8-25 所示。



图 8-24 License 登录平台



图 8-25 iMC 登录页面

在新页面中输入 admin 的密码，选择“使用 License 文件对产品进行注册”，并单击“下一步”按钮，如图 8-26 所示。



图 8-26 选择操作

在下一步的页面中根据页面提示上传 License 文件，并单击“确定”按钮，即完成产品注册。

之后需重启 iMC 服务，授权才正式生效。

(6) 找回授权

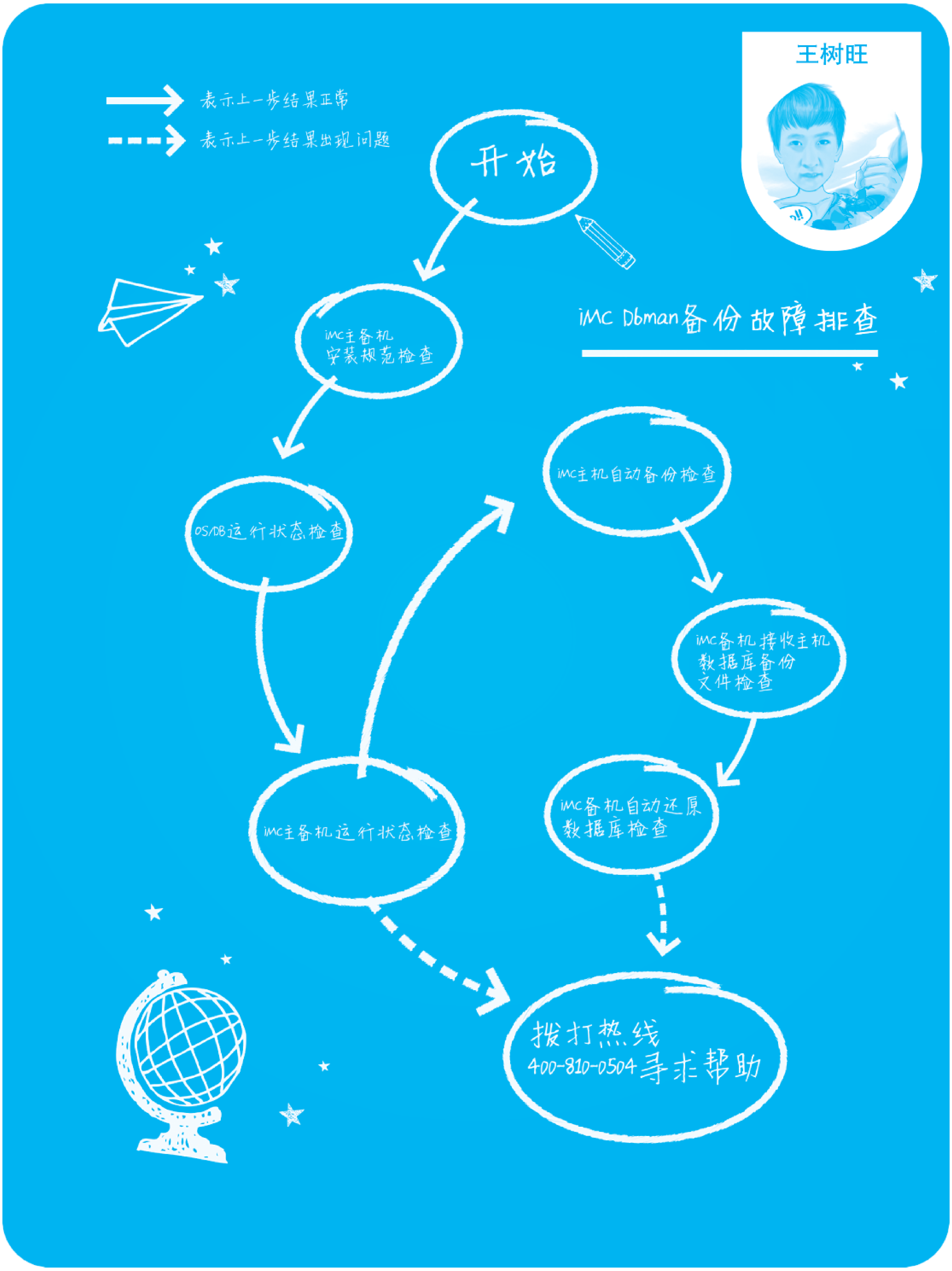
在授权信息或 License 文件丢失时，一般情况下，分销授权应联系市场接口人进行找回，行业用户授权通过 License 平台进行找回处理，如通过 License 平台找回授权码，应提供订单号、未遗失的软件条码，说明需补发电子件或授权函纸件，并说明补发原因。如以上途径不能找回，可联系技术支持中心协助找回，在联系时，应提供最终用户信息、注册时间及平台和组件信息。

(7) 服务器变更

更换服务器可以在 License 平台中单击“设备更换授权变更管理”→“设备更换授权变更申请”命令，进行操作，在操作前应准备好客户承诺书以及新老服务器的 hostid。

(8) 扩容

扩容是指对增加或修改原服务器的授权节点数或功能授权，并生成新的 License 文件的过程，该操作过程在 License 平台上执行。


王树旺
表示上一步结果正常
表示上一步结果出现问题
开始
iMC Dbman备份故障排查
iMC主备机安装规范检查
OS/DB运行状态检查
iMC主备机运行状态检查
iMC主机自动备份检查
iMC备机接收主机数据库备份文件检查
iMC备机自动还原数据库检查
拨打热线 400-810-0504寻求帮助

1. 开始

iMC Dbman 备份是一种冷备方案，在 iMC 的实际安装部署中有着广泛的应用。iMC Dbman 的问题排查思路主要分为如下三大部分。

① iMC 主机能否自动将自己的数据库文件正常备份至本地。

② iMC 主机能否正常将备机出来的数据库文件 FTP PUT 到备机。

③ iMC 备机收到主机 FTP PUT 过来的数据库文件后能否正常还原到备机的 iMC 数据库中。

2. 流程图相关操作说明

(1) iMC 主备机安装规范检查

对照《智能管理中心(iMC)部署和硬件配置方案》对现场 iMC 服务器的安装规范进行检查，排查现场的服务器硬件条件是否符合 iMC 服务器的安装规范要求。重点检查如下几点。

① iMC 服务器是否专机专用，即除了安装 iMC 之外不安装其他类似的网络管理类产品。

② 服务器的硬件配置符合 iMC 的安装及运行要求。

③ 在大规模场景中，iMC 服务器是否进行了合理的分布式部署。

(2) OS/DB 运行状态检查

iMC 作为一个软件产品其运行依赖于底层操作系统及数据库的正常运行，这部分重点排查的内容如下。

① 操作系统、数据库是否为正版软件。

② 操作系统、数据库是否已打上所需的补丁(对照 iMC PLAT 的版本说明书)。

③ 操作系统的系统时间配置正确。

(3) iMC 运行状态检查

这部分重点排查的内容如下。

① iMC 部署监控代理中各进程运行正常，无状态异常的进程。请注意某些情况下管理员可能会出于管理的考虑将某些 iMC 进程配置为手工启动，这种情况是正常的，但 dbman.exe 必须配置为自动启动并且处于运行状态。

② iMC 主、备服务器的 CPU、内存利用率正常。

③ iMC 主备机安装部署的组件、版本及补丁版本必须是相同的。

(4) iMC 主机自动备份检查

检查 iMC 主机部署监控代理的配置，如图 8-27 所示。重点关注如下几项。

① 主机的操作类型应为“自动备份操作”。

② FTP 服务器的 IP 地址、用户名及密码参数须正确无误。

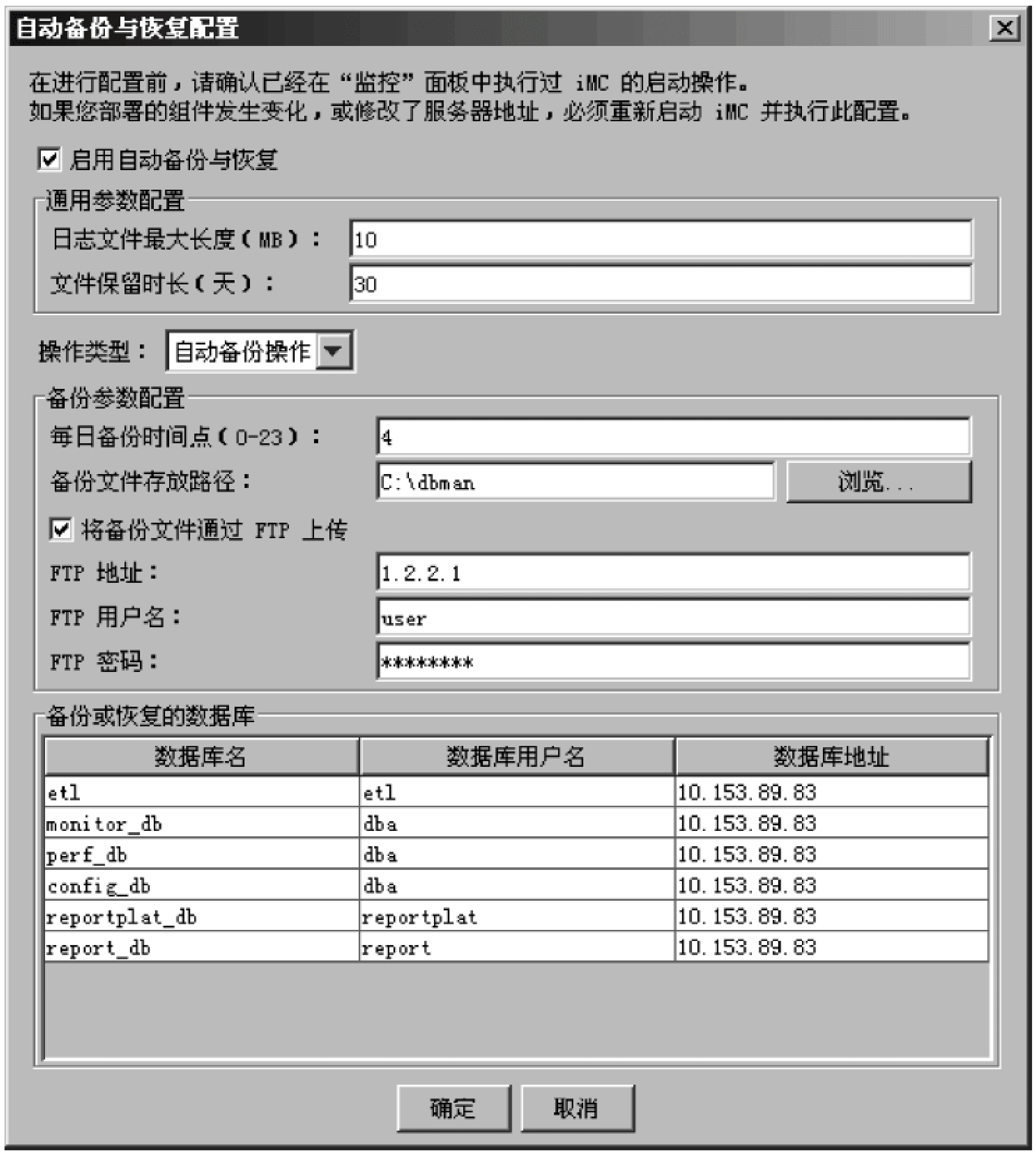


图 8-27　iMC 主机部署监控代理配置

（5）iMC 备机接收主机数据库备份文件检查

检查一下备机的数据库是否存在。

由于 iMC 主机是通过 FTP Put 的方式将数据库备份上传至备机，所以首先应检查备机的 FTP Server 程序工作是否正常。FTP Server 程序非 H3C 厂家产品，请参照对应的厂家的手册进行检查。

其次还可以在主机上的命令行下手工 FTP Put 一个已经备份好的 iMC 数据库备份文件来测试备机的 FTP 服务是否工作正常、中间是否有防火墙过滤 FTP 的端口等。注意如果没有问题请注意测试完成后将对应的 FTP Put 到备机上的测试文件删除。

（6）iMC 备机自动还原数据库检查

iMC 备机部署监控代理请重点检查如下内容。

① 操作类型应配置为“自动恢复”。

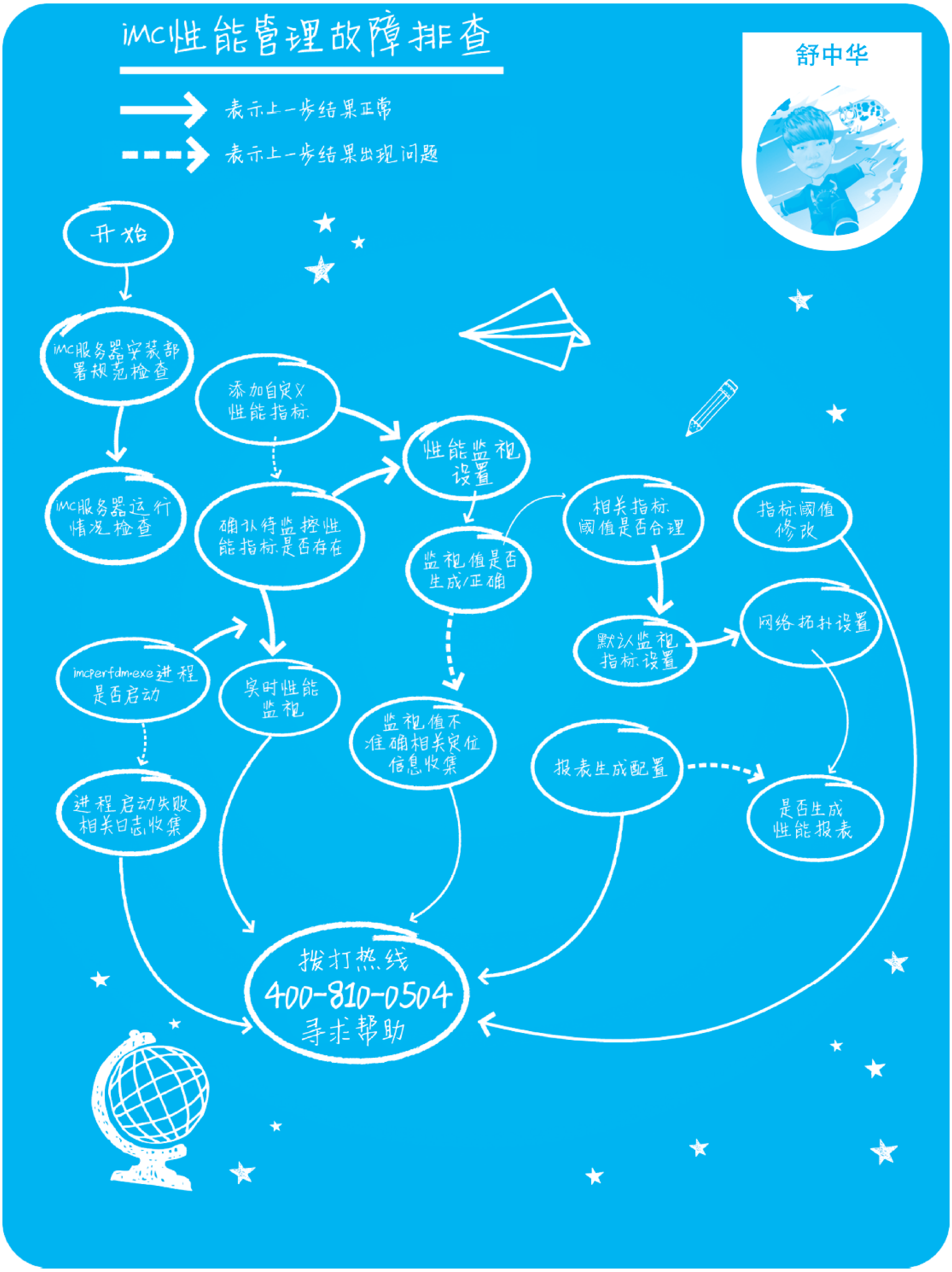
② 数据恢复文件存放路径应与 iMC 备机 FTP 服务器的接入文件目录一致。

③ iMC 备机还原数据库后将原始的数据库备份文件保存在“文件备份路径”下，该路径必须配置为与“数据恢复文件存放路径不一致”并且应有足够的磁盘空间。

图 8-28 所示为 iMC 备机的自动备份与恢复配置。



图 8-28　自动备份与恢复配置


iMC性能管理故障排查
表示上一步结果正常
表示上一步结果出现问题
舒中华
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
添加自定义性能指标
确认待监控性能指标是否存在
性能监视设置
监视值是否生成/正确
相关指标阈值是否合理
指标阈值修改
默认监视指标设置
网络拓扑设置
imcperfdm.exe进程是否启动
实时性能监视
进程启动失败相关日志收集
监视值不准确相关定位信息收集
报表生成配置
是否生成性能报表
拨打热线
400-810-0504
寻求帮助

08 iMC 管理软件 > 8.1 业务软件：iMC > 8.1.6 iMC 性能管理故障排查 > 步骤详解

1. 开始

性能管理特性主要对网络环境进行监视，收集监视数据，并提供灵活的、丰富的数据查看方式，便于用户及时掌握网络运行状况。本流程主要详述了性能管理的配置过程以及针对该应用中可能出现的问题做一说明。

2. 流程图相关操作说明

（1）iMC 服务器安装部署规范检查

iMC 服务器在网顺利运行的前提之一便是 iMC 服务器的安装部署符合相关规范。该过程主要检查 iMC 服务器的物理性能是否足够承载相关业务，重要组件是否分布式部署。相关部署要求规范请参考《智能管理中心（iMC）部署和硬件配置方案》。

（2）iMC 服务器运行情况检查

在 iMC 及其组件的部署符合相关规范的前提下，需要对 iMC 服务器的运行情况进行检查。该过程检查服务器的 CPU/内存利用率是否正常、数据库运行是否正常以及 iMC 是否有未启动进程。

（3）imcperfdm. exe 进程是否启动

可在服务器上执行如下命令行。

tasklist | findstr imcperfdm. exe，如图 8-29 所示。



图 8-29　查 imcperfdm. exe 进程是否启动执行的命令

或者在任务管理器中查看该进程是否运行，如图 8-30 所示。



图 8-30　在任务管理器中查 imcperfdm. exe 进程是否启动

说明：如果未在任务管理器中查看到相关进程，请检查“显示所有用户进程”是否勾选。

(4) 进程启动失败相关日志收集

如果 imcperfdm.exe 进程并未启动，请收集\iMC\server\conf\log 目录下 imcperfdm 开头的日志并反馈。

(5) 实时性能监视

实时性能监视是采用折线图显示用户指定的性能监视项的统计信息，并定时刷新界面显示的数据。实时性能监视功能可以帮助网络管理人员了解设备的当前运行状态，以便于网络管理人员在紧急情况下采取必要措施。相对于 V5 版本的 iMC，V7 版本的实时性能监控固定采集间隔为 5S。以端口输入/输出带宽利用率为例，通过依次单击“资源”→“性能管理”→“实时性能监视”命令，在图 8-31 中填写相关信息，即可完成一个实时性能监控实例的创建工作。



图 8-31 实时性能监控实例的创建工作

新创建的实时性能监控实例效果如图 8-32 所示。

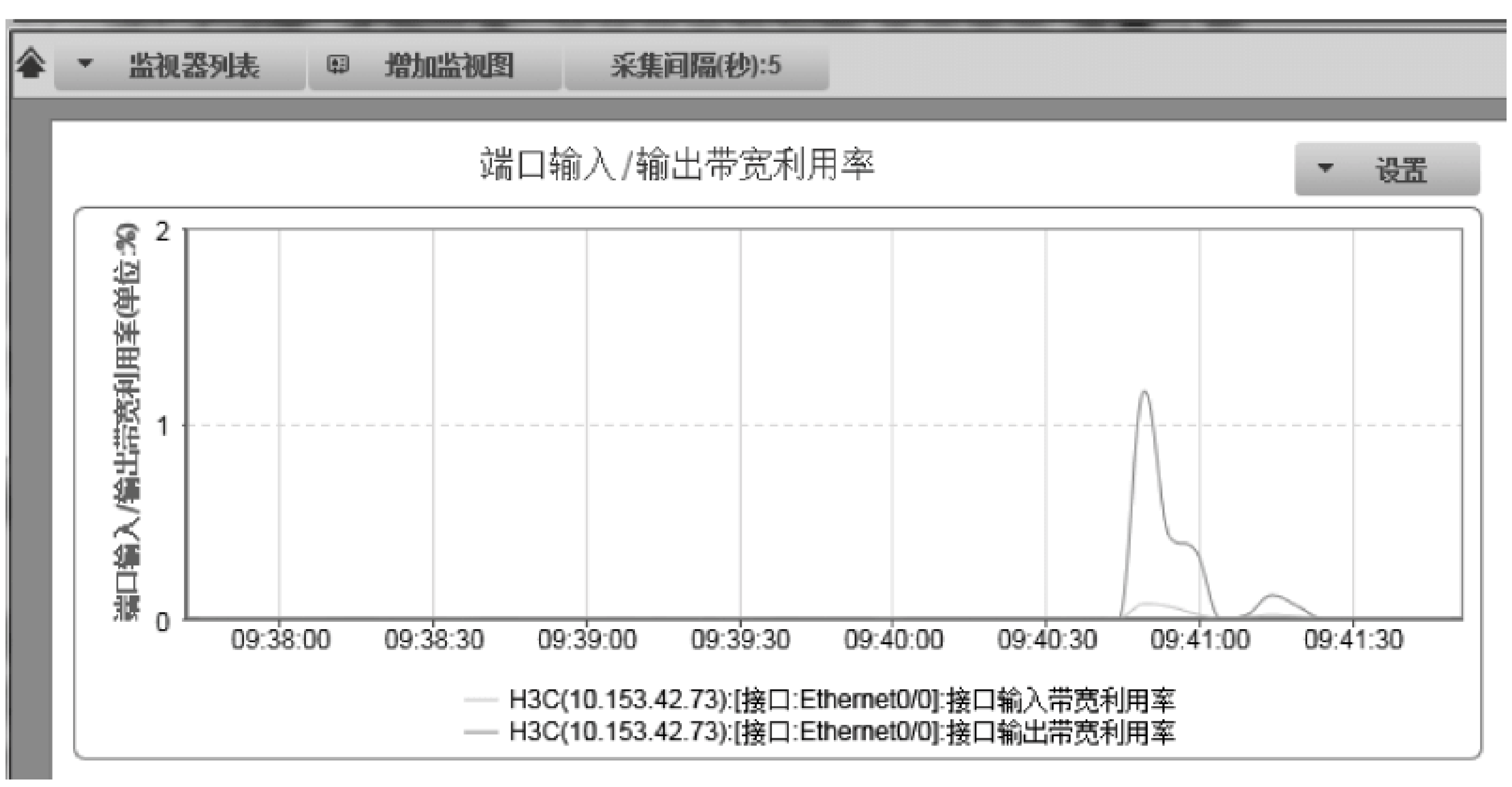


图 8-32 新创建的实时性能监控实例效果

说明：实时性能监控的数据并未写入数据库，iMC 前台页面直接从后台读取数据，当该实时监控页面关闭之后，所有的实时监控数据将不会保存，再次打开时将重新计数。

（6）确认待监控性能指标是否存在

进行性能监控的前提便是该性能监控指标在 iMC 中已经定义，通过依次单击“资源”→“性能管理”→“全局指标设置”，从该页面便可查看 iMC 已经定义的性能监控指标。

说明：iMC 预定义性能监控指标主要针对的是 H3C 设备，主要原因是诸多性能监控指标值均通过读取 MIB oid 获取，且大部分 MIB oid 均为 H3C 私有 MIB。所以再针对第三方厂商设备做性能监控任务时须将具体的监控指标反馈技术支持中心以便确认是否支持。

（7）添加自定义性能指标

iMC 针对第三方厂商设备或 H3C 设备可能存在相关性能监控指标未先定义的情况，可以通过自定义性能监控指标解决该问题。通过依次单击“资源”→“全局指标设置”→“增加自定义性能指标”命令来定义一个新的监控指标，如图 8-33 所示。



图 8-33　定义一个新的监控指标

自定义性能监控指标的过程也可参考 KMS 22253。

说明：自定义性能监控指标目前只支持 MIB 返回值为整型的 OID，查看 MIB 返回值，可以查看 MIB 定义文件，如下为 Base syntax 字段。

Name：ifMtu

Type：OBJECT-TYPE

OID：1.3.6.1.2.1.2.2.1.4

Full path：iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).interfaces(2).ifTable(2).ifEntry(1).ifMtu(4)

Module：IF-MIB

Parent：ifEntry

Prev sibling：ifType

Next sibling：ifSpeed

Numerical syntax：Integer (32 bit)

Base syntax：Integer32

(8) 性能监视设置

在确定相关需要监控的性能监视实例之后，通过依次单击“资源”→“性能管理”→“监视设置”→“增加监视”命令，就可以对相关设备进行性能监控，如图 8-34 所示。



图 8-34　相关设备的性能监控

说明：该处选择“监视设备”与“监视实例”的区别在于监视实例可以选择监视的单个实例，而监视设备则不支持选择监视的实例，默认会将符合条件的某指标所有实例都做监控。

(9) 监视值是否生成/正确

在成功创建性能监控指标之后，便可查看该性能监控指标对应的值，通过依次单击“资源”→“性能管理”→“监视设置”命令，单击功能按钮便可查看，如图 8-35 所示。



图 8-35　性能监控指标对应的值

也可通过单击实例数，来查看单个实例的数据。

(10) 监视值不准确相关定位信息收集

如果在应用中发现 iMC 性能监控结果与设备上通过命令行查看打印出来的值偏差很大，

请在 iMC 服务器抓取与该设备的交互报文 10～15min，并将 iMC 性能监控结果截图与设备命令行打印结果一起反馈技术支持中心。

（11）相关指标阈值是否合理

在 iMC 全局指标设置中，针对每个性能监控指标都做了默认的阈值设置。在现网应用中，可能出现该指标不符合现网要求的情况，iMC 支持对该指标阈值进行修改。

（12）指标阈值修改

指标阈值支持通过全局和单个监控实例两种方式进行修改。

全局方式修改。依次单击“资源”→“全局指标设置”命令，并双击对应的监控指标，便可进行修改，以 CPU 监视为例，如图 8-36 所示。



图 8-36　全局方式修改

单个监控实例修改。依次单击“资源”→“性能管理”→“监视设置”命令，在相关设备操作列单击“修改属性”按钮，便可进行修改，如图 8-37 所示。

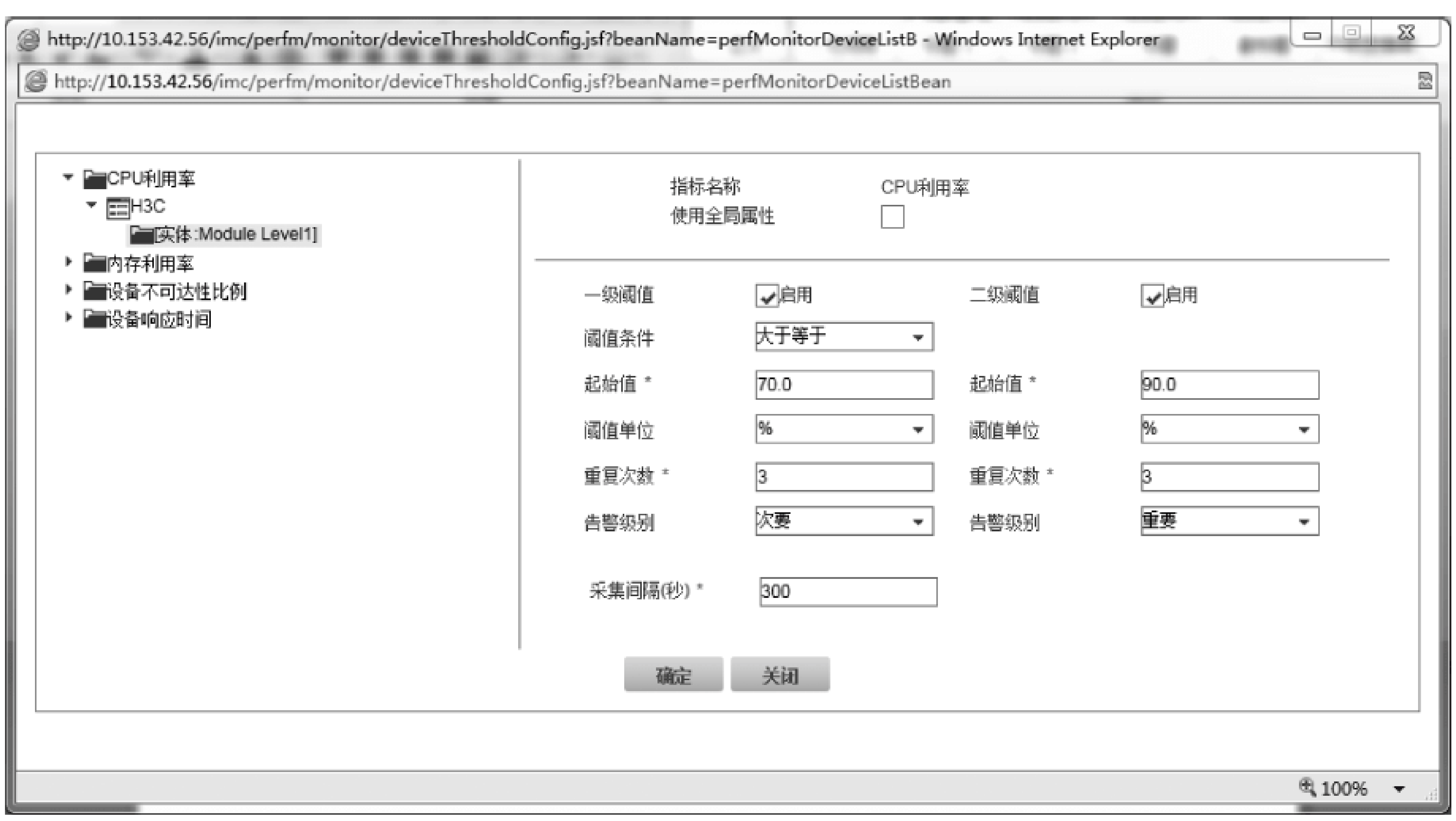


图 8-37　单个监控实例修改

(13) 默认监视指标设置

默认监控指标是指设备在加入到 iMC 平台之后 iMC 自动对其创建的性能监控任务。iMC 默认监控 CPU 利用率、内存利用率、设备响应时间以及设备不可达性比例。可以通过依次单击“系统管理”→“系统配置”→“默认监视指标”命令来进行定义，如图 8-38 所示。



图 8-38　默认监视指标设置

(14) 网络拓扑设置

该功能用于增加或修改网络拓扑参数以便在自定义拓扑中可以查看相关性能监控值，可以通过依次单击“资源”→“网络拓扑设置”命令来设置网络拓扑，相关限制请参考联机帮助，如图 8-39 所示。



图 8-39　网络拓扑设置

(15) 是否生成性能报表

iMC 支持将性能监控结果通过报表的形式导出，导出方式支持周期报表和手工下载两种，具体导出方式详见(16)。

(16) 报表生成配置

周期报表方式。依次单击“报表”→“增加周期报表”命令，便可增加对应的周期报表，相关信息请参考联机帮助，如图 8-40 所示。



图 8-40　周期报表生成配置

手工导出方式。依次单击“资源”→“性能管理”→“性能视图”命令，选定对应的性能视图，单击“报表”按钮便可将报表生成导出，如图 8-41 所示。

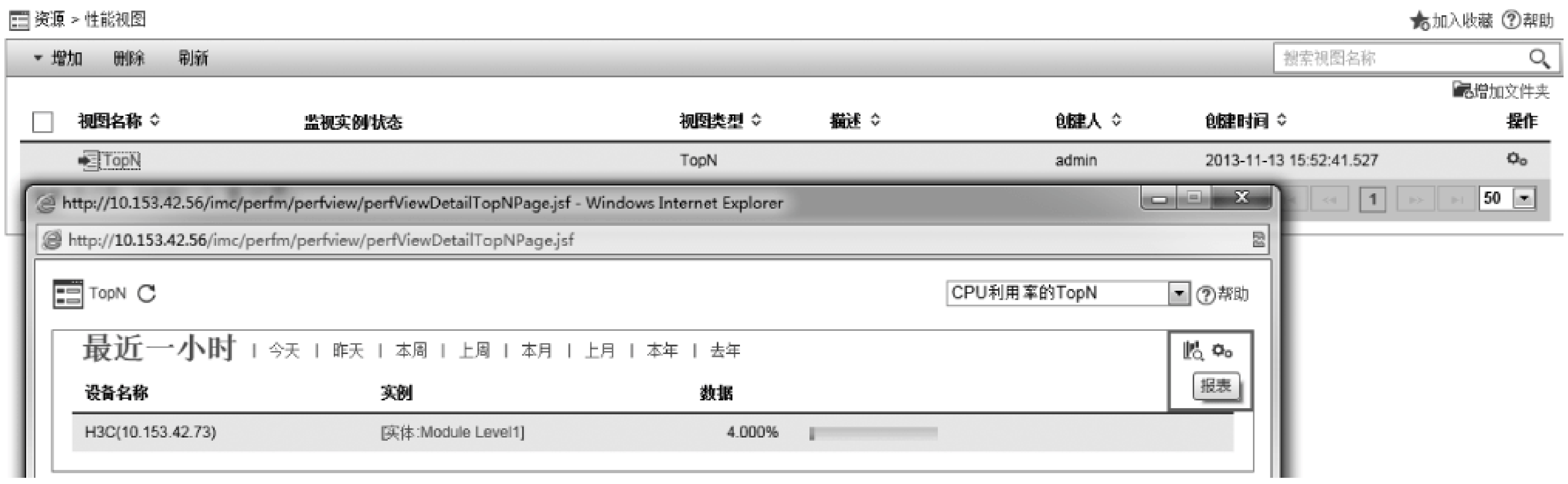
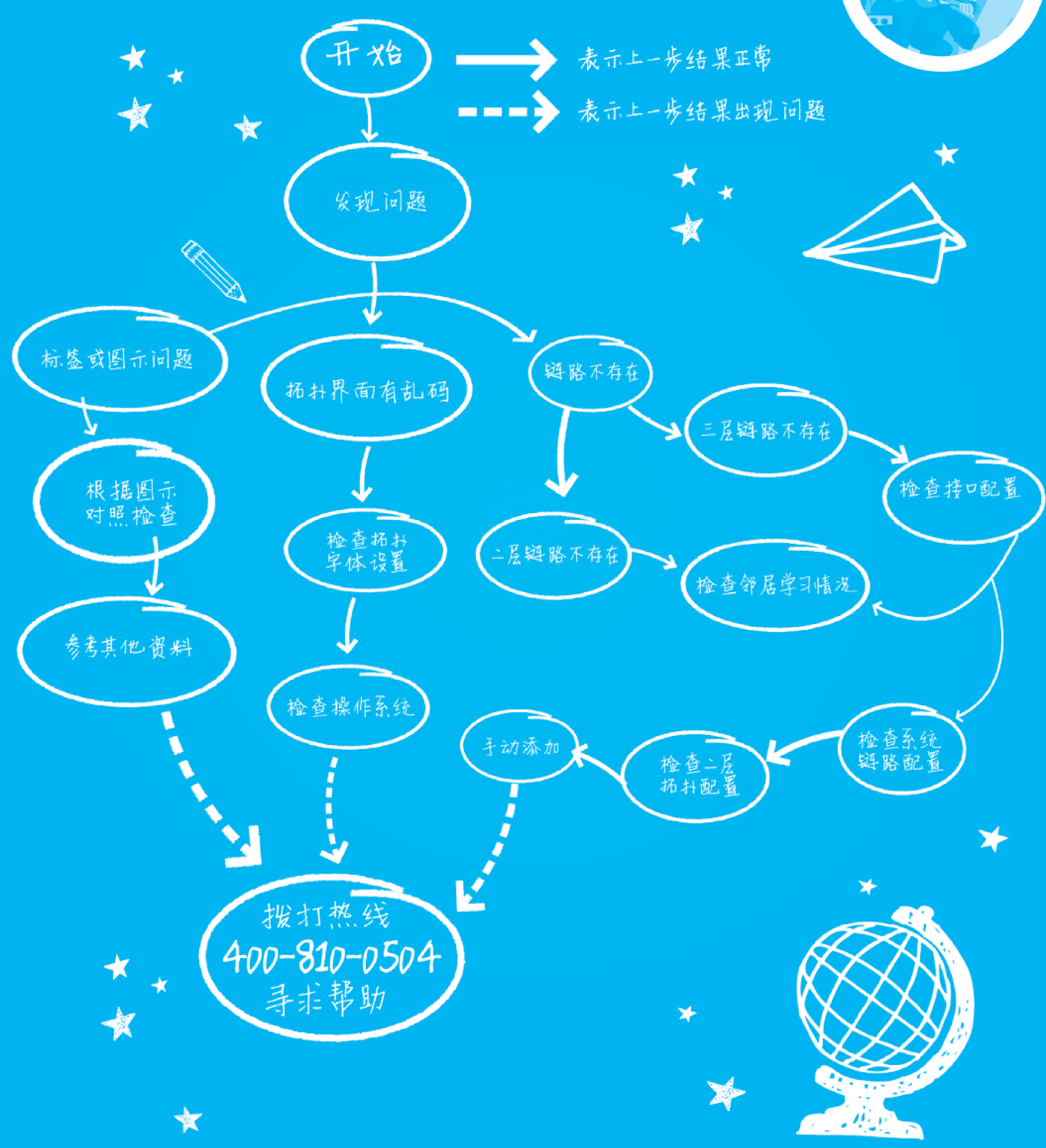


图 8-41 手工导出方式

王剑虎

iMC拓扑管理故障排查



1. 拓扑管理

iMC 拓扑用于运维时查看全网拓扑或自定义拓扑。

在该流程中，将对拓扑管理中常见问题一般为各类标签或字体的疑问，另一类为链路问题，下面将对这两类问题的排查流程进行说明。

2. 流程图相关操作说明

（1）发现问题

说明：拓扑作为运维观察的首要切入点，很有可能是最先发现问题之处，但不是所有在拓扑上看到的问题根源都在拓扑本身上，本流程将根据不同问题做相关指引。

（2）标签或图示问题

当出现与正常不一致的图标或图示及链路颜色类型等情况，应首先根据拓扑图示确认该提示的含义，如图 8-42 所示。



图 8-42　标签或图示问题

单击拓扑上方的红框所示的“图例”按钮，即可进行查看各类图例。

（3）根据图示对照检查

不同的问题对应不同的检查方式，如发现设备提示“？”，根据图例可知为设备不通，此时应在 iMC 服务器上使用 ping 命令检查设备的连通性。

如二层链路为虚线，应检查两端链路的邻居发现协议是否正常及 MAC 学习是否正常。

问题应对症排查，本文不一一举例。

（4）参考其他资料

如上文所述，拓扑是发现问题之处，并不是所有问题之源。因此对于在本流程中发现的非拓扑问题，应参考其他云图或 KMS 等产品资料进行排查。

（5）拓扑界面有乱码

在某些情况下，可能会出现本应为中文的设备标签等信息变为如图 8-43 所示的乱码。

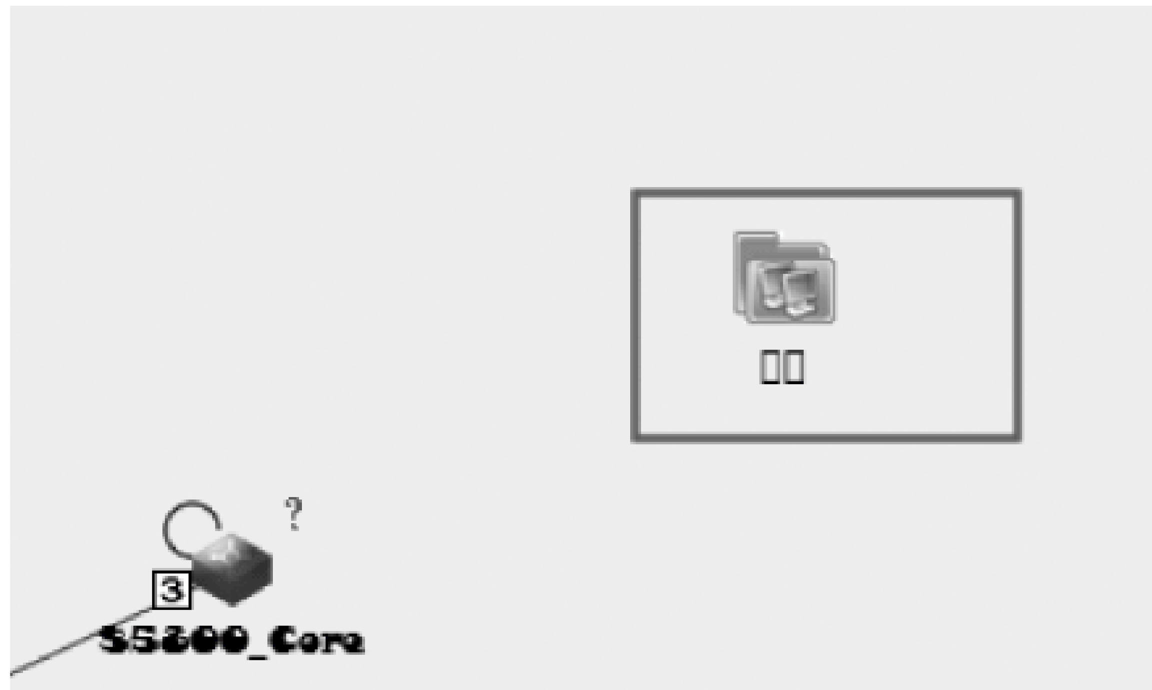


图 8-43　拓扑界面有乱码

(6) 检查拓扑字体设置

此问题多为拓扑字体设置有误导致，在如图 8-44 所示的界面中检查字体的设置是否为中文，如果不是，将其修改为系统字库中存在的中文字体。

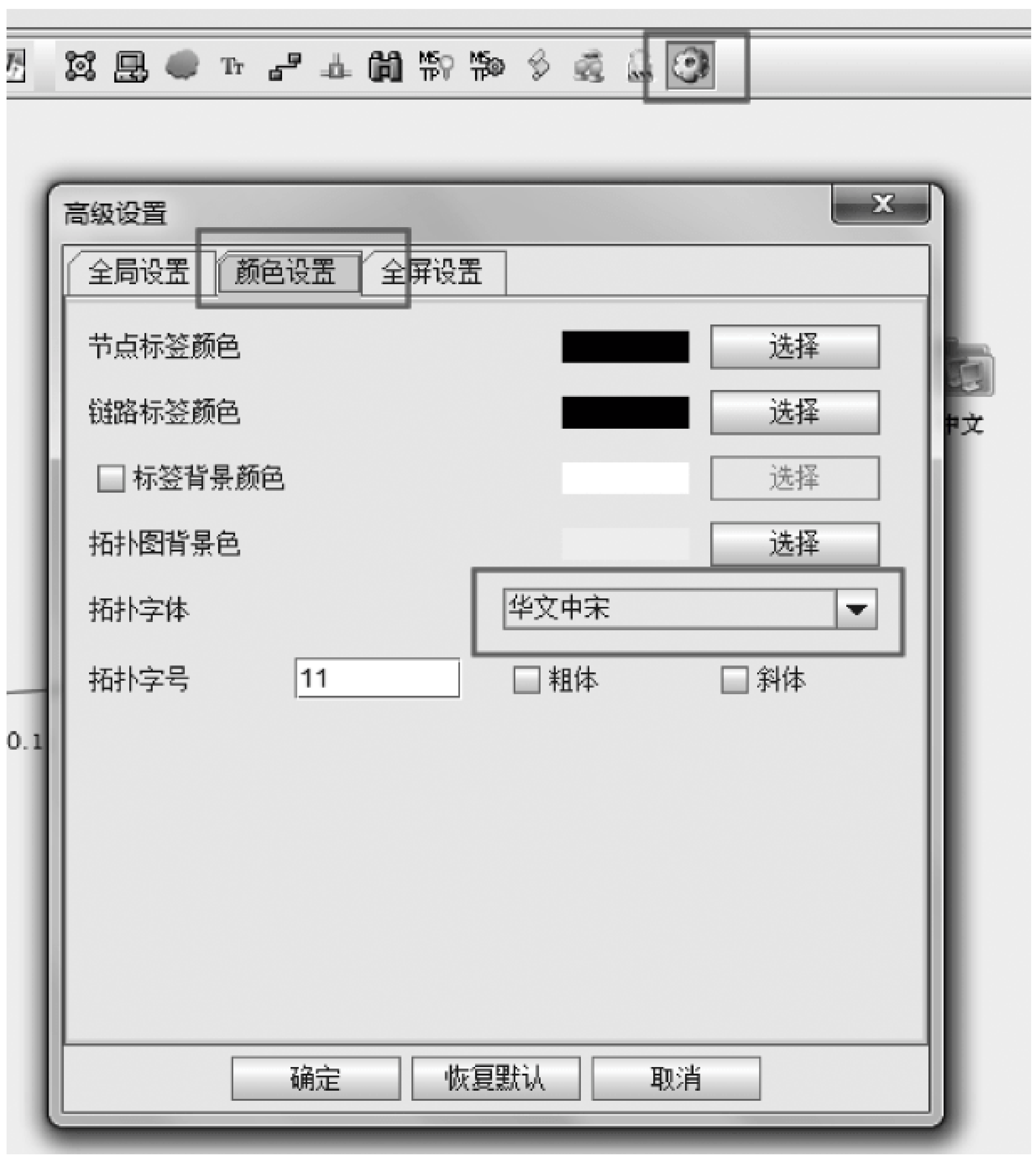


图 8-44　检查拓扑字体设置

(7) 检查操作系统

如设置为中文字体后仍为乱码，则说明系统字库有问题，请检查系统是否为英文操作系统，或盗版汉化不完整的操作系统，或字库文件是否存在。

(8) 链路不存在

iMC 拓扑中的链路分为二层链路和三层链路，有不同的识别方式，但对于三层链路，可以通过设置使其通过二层链路学习进行计算，一般用于当三层链路两侧接口 IP 地址为非 30 位掩码时使用。

(9) 三层链路不存在，检查接口配置

三层链路自动计算的前提条件是两侧接口是 PPP 类型链路或两侧 IP 地址为 30 位掩码。

在此步骤中，请在 iMC 上检查链路两侧的接口上是否符合上述条件。

（10）二层链路不存在，检查邻居学习情况

二层链路在一般情况下是通过 LLDP/NDP/CDP 等邻居发现协议来进行学习计算的。在此步骤中，请在设备上检查链路两侧接口上是否正确学习到了对端的邻居关系。

（11）检查系统链路

当确认以上步骤检查结果正常，如果链路仍然不存在，应检查拓扑的系统链路中，是否做过删除操作，如果是，则应如图 8-45 所示操作确认并将其恢复。

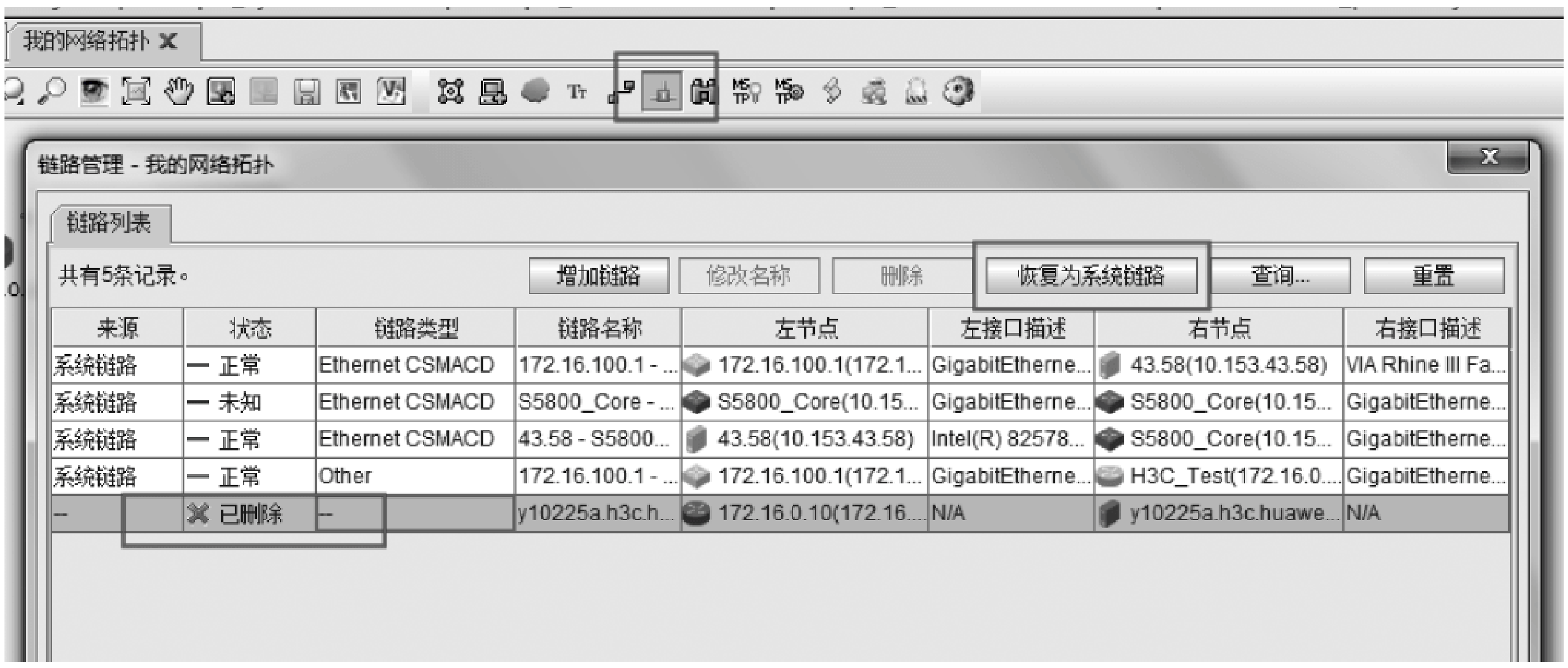


图 8-45　检查系统链路

（12）检查二层拓扑配置

在 iMC 的管理界面中，单击“系统管理→系统配置→系统参数”命令中，找到“二层拓扑配置”，可将该选项中所有项目均配置为“是”，并同步链路两端设备，等待一段时间观察链路是否可以正常学习。注意：要保证 iMC 对设备有 snmp 写权限。

（13）手动添加

在以上检查未果的情况下，可能通过手动添加链路来解决问题。在手动添加的过程中需保证链路和实际设备连接情况相符，否则即使添加了链路也无法正常同步链路状态。添加链路的操作如图 8-46 所示。

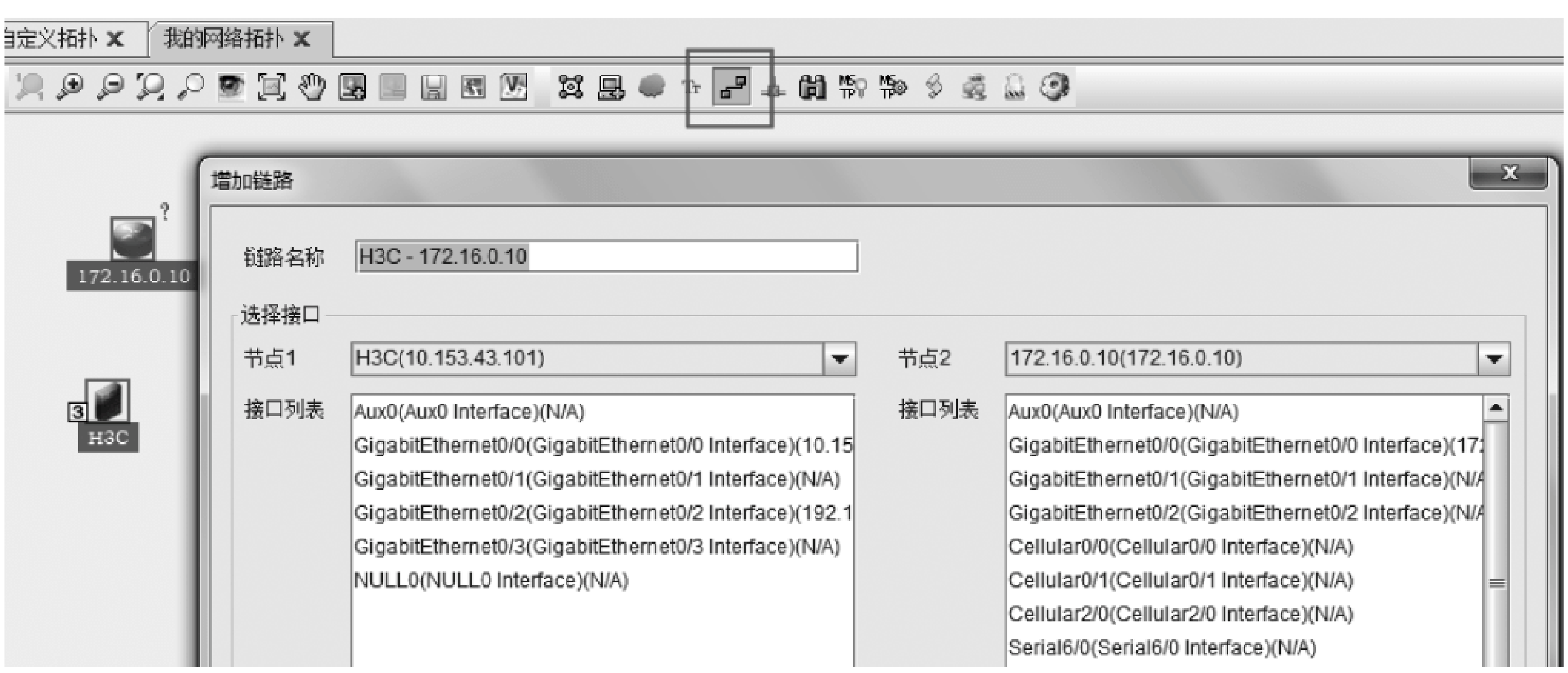
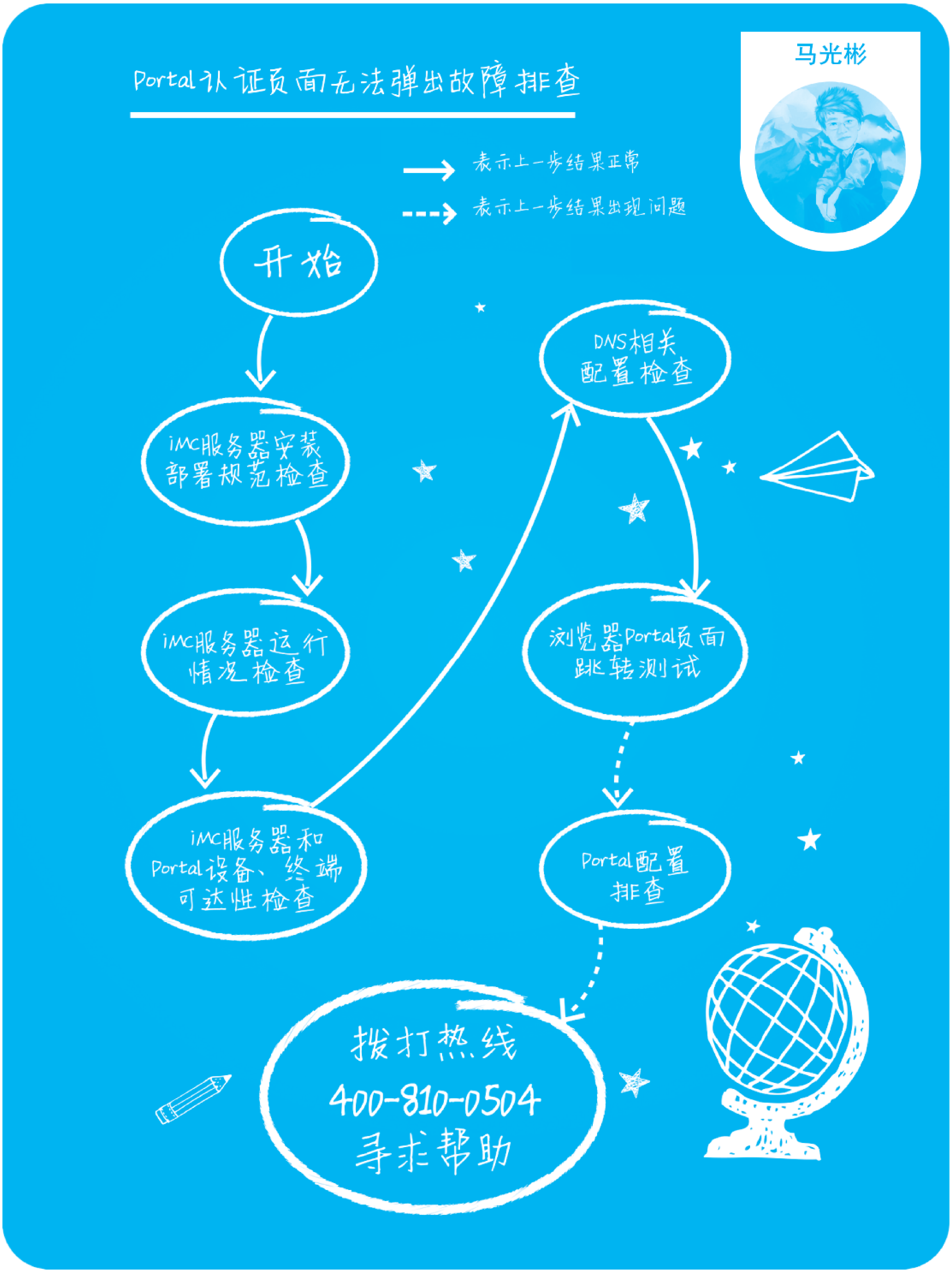


图 8-46　手动添加链路


马光彬
Portal认证页面无法弹出故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和Portal设备、终端可达性检查
DNS相关配置检查
浏览器Portal页面跳转测试
Portal配置排查
拨打热线
400-810-0504
寻求帮助

1. 开始

Portal 认证是一种网页认证，Portal 页面重定向的原理为：认证上线的终端在向外发起 HTTP GET 请求时，网关设备会以配置好的 Portal URL 来填充地址字段，将该 GET 请求重定向到 Portal 服务器上，转而进行 Portal 认证。在使用 iNode 做认证的场景，建议先使用网页调试 Portal 认证。

iMC Portal 认证网页故障排错定位思路：首先检查服务器软硬件及性能是否满足当前认证需要，然后从网页上线的现象来分析，相应做 iMC 服务器的检查、DNS 服务器相关配置的检查和 Portal 相关配置的检查。

本文中举例组网如图 8-47 所示。



图 8-47　组网举例

IP 规划如下。

认证终端 PC：192.168.3.2/24，网关 192.168.3.1。

认证设备 H3C：VLAN 3：1192.168.3.1/24，VLAN 1：192.168.1.104/24。

iMC 服务器：192.168.1.211/24，网关 192.168.1.104。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题时首先需要确认服务器软硬件配置情况是否符合要求。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器对应业务量的配置需求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”各组件是否是已部署的状态。

需要关注的组件有“用户接入管理”和“Portal 服务器”，其状态都应为“已部署”，如图 8-48 所示。

(2) iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中“进程”选项卡中是否有未启动的进程，各进程是否正常为“已经启动”。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

组件名	描述	版本	状态	部署位置
智能管理平台 - 虚拟资源管理	对虚拟资源进行管理。	iMC PLAT 7.1 (E03...	已部署	主服务器
智能策略服务代理	提供统一的策略服务代理功能，...	iMC ISP 7.1 (E0302)	已部署	主服务器
用户接入管理 - 用户接入管理	提供对接入用户、接入业务的配...	iMC UAM 7.1 (F0303)	已部署	主服务器
用户接入管理 - Portal服务器	提供Portal认证功能。	iMC UAM 7.1 (F0303)	已部署	主服务器
用户接入管理 - EIP服务器	提供终端智能识别的功能。	iMC EIP 7.1 (F0303)	已部署	主服务器
用户接入管理 - EIP从服务器	部署在EIP服务器之外的其他服...	iMC EIP 7.1 (F0303)	未部署	
用户接入管理 - 策略服务器	提供安全认证的功能。	iMC UAM 7.1 (F0303)	已部署	主服务器
用户接入管理 - 策略代理服务器	提供对安全认证报文的转发功能。	iMC UAM 7.1 (F0303)	已部署	主服务器
用户接入管理 - 用户自助服务	提供用户资料的自助查询和维护...	iMC UAM 7.1 (F0303)	已部署	主服务器
自主页面定制Web服务器	提供一个独立的Web容器，用于...	iMC UAM 7.1 (F0303)	已部署	主服务器
用户接入管理 - Portal服务器	提供Portal认证功能。	iMC UAM 7.1 (F0303)	未部署	
用户接入管理 - 策略代理服务器	提供对安全认证报文的转发功能。	iMC UAM 7.1 (F0303)	未部署	
自主页面定制Web服务器	提供一个独立的Web容器，用于...	iMC UAM 7.1 (F0303)	未部署	
EAD安全策略管理 - 安全策略管理...	提供对EAD业务的配置功能。	iMC EAD 7.1 (E0301)	已部署	主服务器
EAD安全策略管理 - 桌面资产管理	提供对桌面资产业务的配置和用...	iMC EAD 7.1 (E0301)	已部署	主服务器
EAD安全策略管理 - 桌面资产管理...	提供对桌面资产管理报文的转发...	iMC EAD 7.1 (E0301)	已部署	主服务器
智能管理平台 - 服务器资源管理	对网络中的服务器资源进行管理。	iMC SSA 7.1 (E030...	已部署	主服务器
应用管理	用于监视不同种类业务的应用程...	iMC APM CONFIG 7....	已部署	主服务器
应用管理服务	用于采集不同种类业务的应用程...	iMC APM 7.1 (E0303)	已部署	主服务器
应用管理服务	用于采集不同种类业务的应用程...	iMC APM 7.1 (E0303)	未部署	

请选择组件，按下鼠标右键激活操作菜单。

图 8-48　iMC 服务器安装部署规范检查

① 打开部署监控代理，查看 uam.exe、portalserver、webServiceNode1、webServiceNode2、uamjob 进程是否正常启动。另外，如果是网页 Portal 认证还需要确认 Portal 服务器上的 jserver/webserver 进程是否正常启动，如图 8-49 所示。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
img.exe	已经启动	本机	0	7,628	2015-04-01 15:46:02	核心进程	自动
tftpserver.exe	已经启动	本机	0	14,772	2015-04-01 15:47:28	可管理进程	自动
uam.exe	已经启动	本机	0	26,560	2015-04-03 22:29:29	可管理进程	自动
apmserver	已经启动	本机	0	216,424	2015-04-01 15:45:23	可管理进程	自动
damserver	已经启动	本机	0	241,188	2015-04-01 15:45:37	可管理进程	自动
euplat	已经启动	本机	0	321,292	2015-04-01 15:45:37	可管理进程	自动
ispserver	已经启动	本机	0	247,108	2015-04-01 15:45:37	可管理进程	自动
cmdbserver	已经启动	本机	0	332,192	2015-04-01 15:45:37	可管理进程	自动
jserver	已经启动	本机	0	2,463,704	2015-04-01 15:45:37	可管理进程	自动
portalserver	已经启动	本机	0	324,748	2015-04-01 15:45:37	可管理进程	自动
webServiceNode1	已经启动	本机	0	317,496	2015-03-31 09:47:15	可管理进程	自动
webServiceNode2	已经启动	本机	0	317,644	2015-04-01 15:45:37	可管理进程	自动
seplat	已经启动	本机	0	315,712	2015-04-01 15:45:37	可管理进程	自动
uamjob	已经启动	本机	0	214,228	2015-04-01 15:45:37	可管理进程	自动
uamThirdAuth	已经启动	本机	0	305,564	2015-04-01 15:46:42	可管理进程	自动
mschapv2server	已经启动	本机	0	310,872	2015-04-01 15:48:54	可管理进程	自动
eipserver	已经启动	本机	0	280,716	2015-04-01 15:45:37	可管理进程	自动
policyserver	已经启动	本机	0	262,016	2015-04-01 15:45:37	可管理进程	自动
difserver	已经启动	本机	0	247,900	2015-04-01 15:45:37	可管理进程	自动
stmserver	已经启动	本机	0	252,204	2015-04-01 15:45:37	可管理进程	自动
acmweb	已经启动	本机	0	310,648	2015-04-01 15:45:37	可管理进程	自动

图 8-49　查看各进程是否正常

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) jserver 是 Portal 组件集中式部署时所需关注的进程；webserver 为 Portal 组件分布

式部署时，在从机上需要确认的进程。

② 检查服务器 1812、1813、50100、50200 UDP 端口是否被 uam 相关进程所监听，如图 8-50、图 8-51 所示。



图 8-50 检查进程监听情况

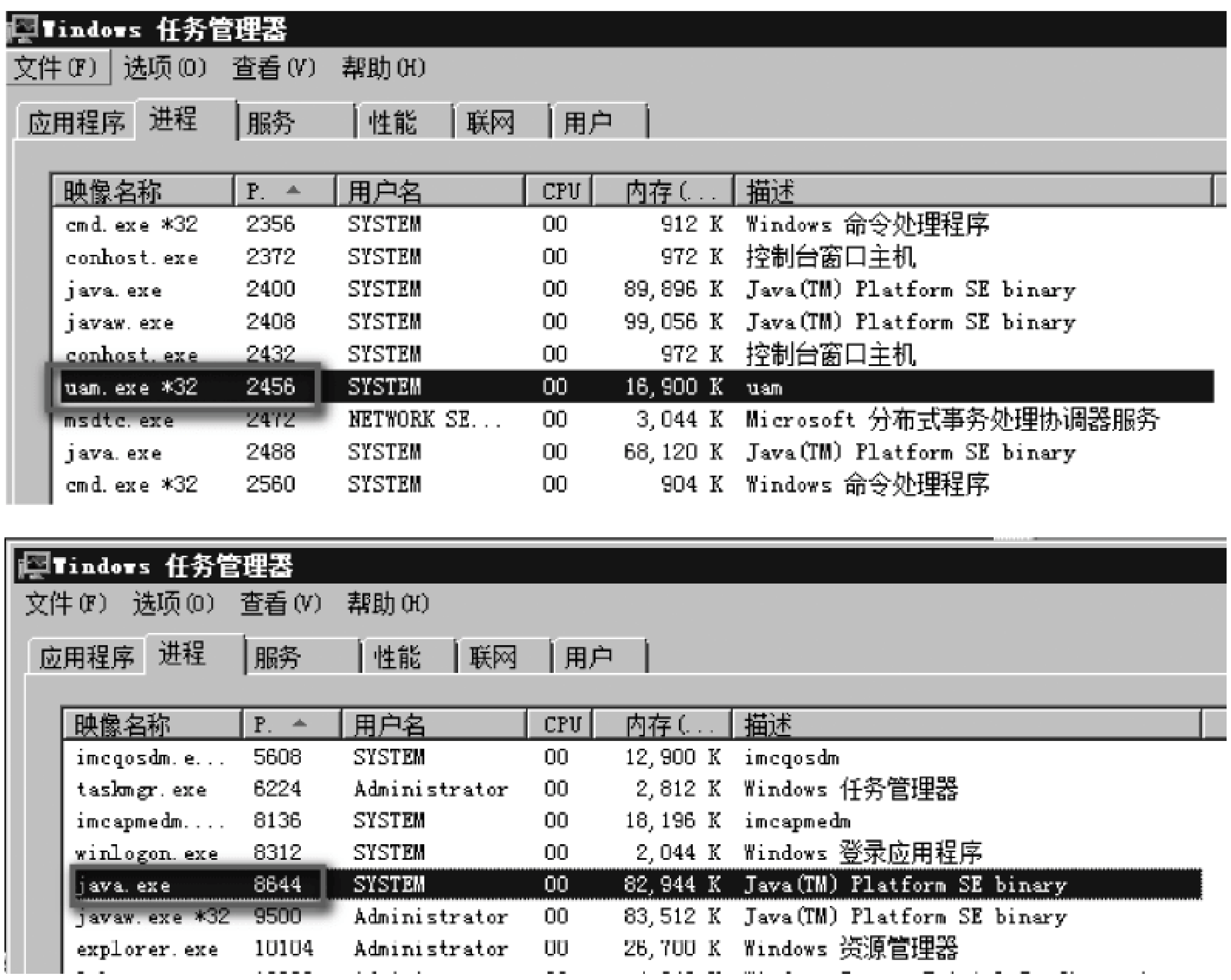


图 8-51 进程查看

说明：

(a) Windows 操作系统中，通过

netstat-aon | findstr ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-52 所示。

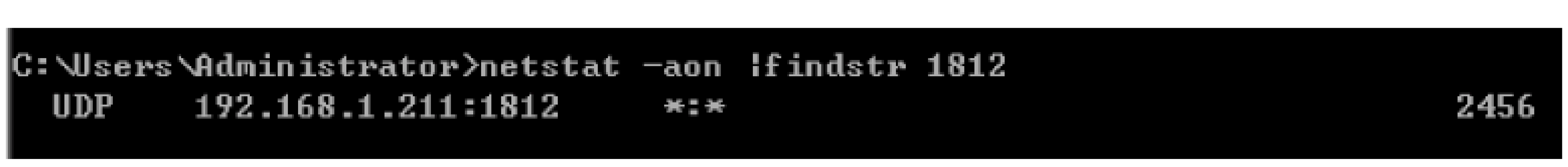


图 8-52 命令提示符回显

其中第一列 UDP 所指监听的协议，第二列 192.168.1.211:1812 所指监听的服务器的 IP 和端口号，第三列 *:* 代表此行信息为监听状态，最右一列 2456 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，1812/1813 端口所对应的应为 uam 相关的进程，50100/50200 所对应的应为 java 进程。

(3) iMC 服务器和 Portal 设备、终端可达性检查

PC 或手机浏览器输入 Portal URL：http://192.168.1.211:8080/portal，看是否正常弹出页面，如果正常弹出说明网络正常；如果不正常则需要排查网络。

① 网络可达性检查。在认证上线之前终端 PC 是可以和 Portal 所在服务器可达的。分别从 iMC 服务器上 ping 接入设备 IP、Portal 设备 IP 和终端 IP。对于本文的组网环境，需要分别测试 192.168.3.2 与 192.168.1.211、192.168.3.1 与 iMC192.168.1.211、192.168.1.104 与 iMC192.168.1.211 之间的双向可达性。

② 检查服务器防火墙是否关闭。

③ 检查网络中防火墙，终端到服务器之间的 8080 端口是否放通。

(4) DNS 相关配置检查

网络调通后，测试 DNS 相关配置是否正常。

如果浏览器输入普通 URL 比如 www.baidu.com 无法弹出页面，而输入任意 IP 地址比如 1.1.1.1 能够正常跳转，说明 DNS 无法正常解析 URL，无法产生 HTTP 流量，导致设备不能触发重定向。此时，看从终端 ping DNS 服务器的地址通不通，如果 DNS 通说明 DNS 解析有问题；如果 DNS 不通就需要调整网络调通。

① 终端到 DNS 不通，首先检查是否路由可达；然后配置免认证规则，放通终端到 DNS 通信，配置命令为：portal free-rule 0 source ip any destination ip 8.8.8.8 mask 255.255.255.255。

② 终端到 DNS 通但无法解析：排查 DNS 服务器解析问题(比如 ping www.baidu.com 不通，ping 百度的公网地址能通，说明 DNS 解析出了问题)。

如果浏览器输入 IP 地址 1.1.1.1 也无法弹出页面，则查看设备上配置的 Portal URL 是否写正确，不正确修改之，正确则确认接口是否启用 Portal，如果已经启用，则说明设备重定向有问题，咨询设备侧。

```
[H3C] display current-configuration | include portal serverimc
portal server imc ip192.168.1.211 key 123 url http://192.168.1.211:8080/portal
portal server imc method direct
```

说明：

(a) 其中 imc 为设备本地有效的 Portal 服务器名称，192.168.1.211 为 Portal 服务器的地址，123 为 Portal 设备和 Portal 服务器交互时所用的共享密钥，http://192.168.1.211:8080/portal 为 Portal 网页的重定向 URL。

(b) 对于命令 portal server imc method direct，需要详细检查其是否在认证接口上启用。

(5) Portal 配置排查

经过以上步骤的排查，一般情况下 Portal 页面都会正常弹出，但有时也会有报错：Portal 服务器获取不到设备信息或设备没有回应 req-info 报文。实际上目前实现和发送 req_info 已关系不大，所以出现此错误基本可以确认是根据用户地址找不到对应 Portal 设备信息，如

图 8-53 所示,有可能由以下原因导致。



图 8-53　找不到对应 Portal 设备信息

① 用户上线 IP 地址没有包含在 iMC 的 Portal IP 地址组网段中。本案例用户认证网段为 192.168.3.0/24,如果终端获取的地址不在该网段,则无法弹出页面,如图 8-54 所示。



图 8-54　本案例用户认证网段

② 检查设备的 sysname 是否含有中文或特殊字符。

③ iMC 没有配置端口组,或者端口组中引用的地址组不正确。本案例 IP 地址组名称为 vlan3,如图 8-55 所示。



图 8-55　本案例地址组名称

④ 使用移动终端等上线，IP地址经常变化，而由于Portal具有缓存机制，因此，造成缓存中原地址和现有报文头地址不一致（分别对应私网地址属性和公网地址属性），被识别为NAT，从而无法匹配到对应的地址组。此时应清空浏览器缓存测试，如图8-56所示。

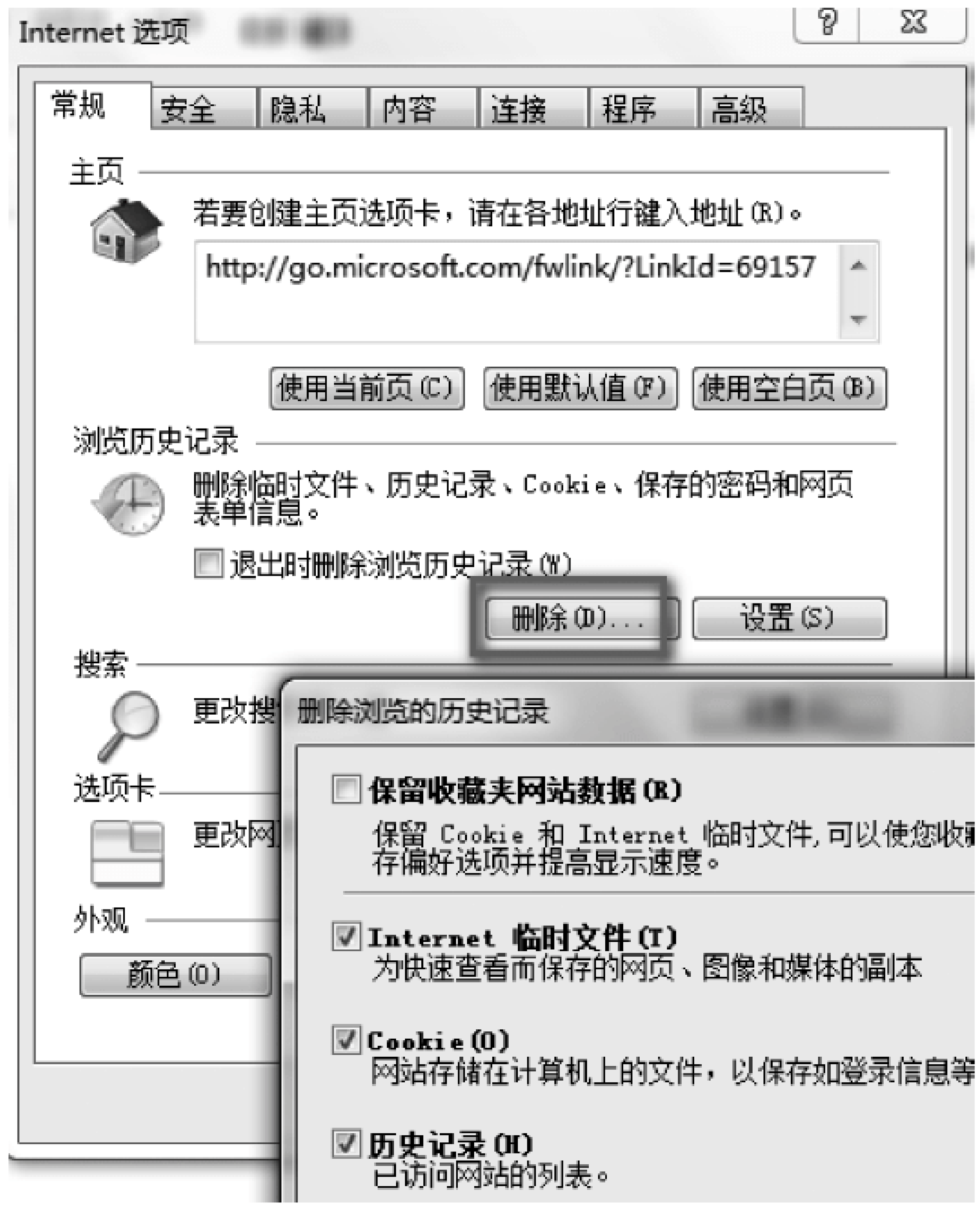
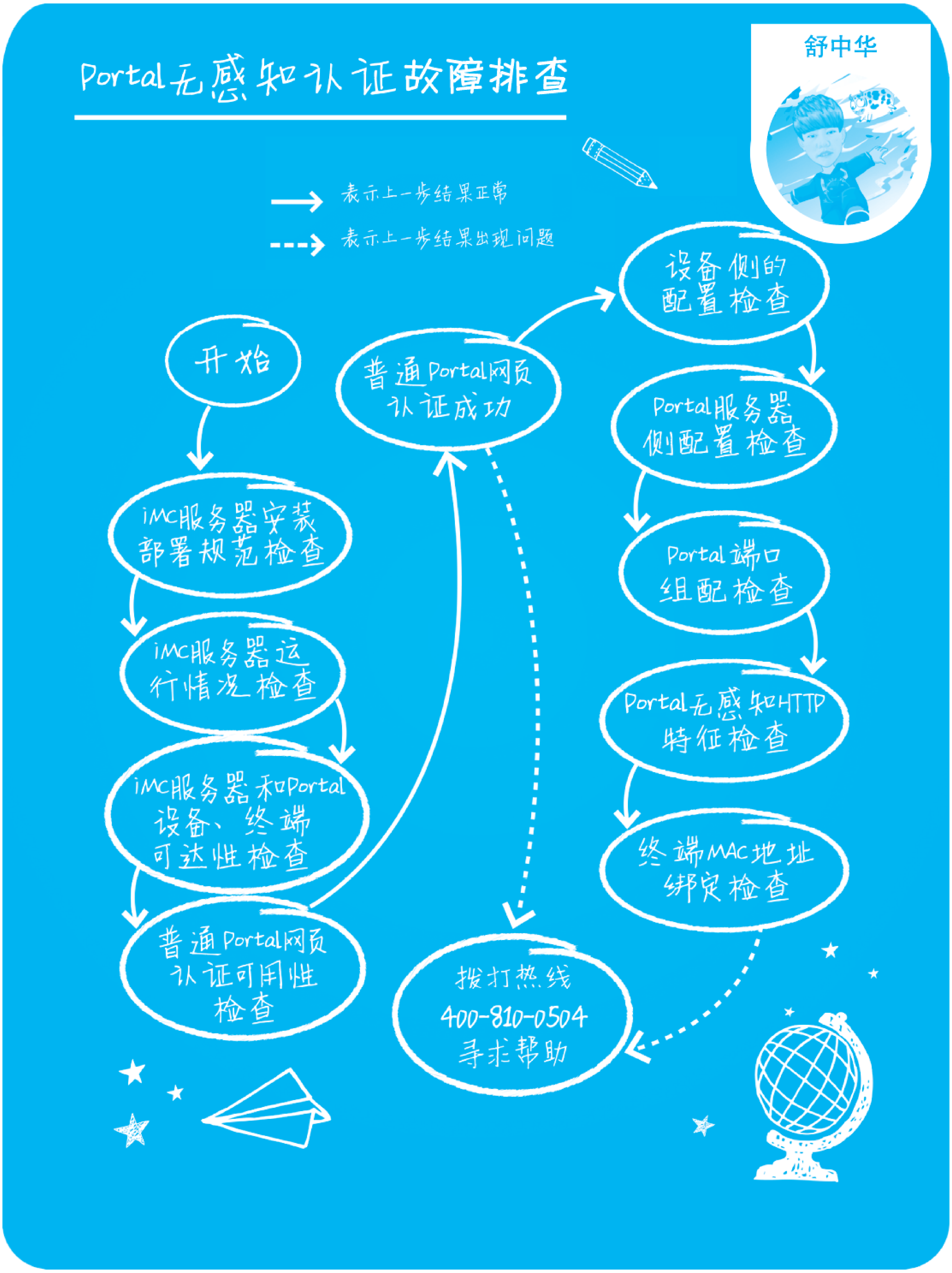


图8-56　清空浏览器缓存测试

⑤ 配置台配置没有生效，即通知Portal服务器加载失败，造成这种情况原因可能是Portal服务器未正常启动或50900端口没有正常绑定，可以查看如图8-57所示界面Portal主页信息显示正常与否来确认50900端口是否正常工作。



图8-57　Portal主页信息



Portal无感知认证故障排查
舒中华
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和Portal设备、终端可达性检查
普通Portal网页认证可用性检查
普通Portal网页认证成功
设备侧的配置检查
Portal服务器侧配置检查
Portal端口组配置检查
Portal无感知HTTP特征检查
终端MAC地址绑定检查
拨打热线 400-810-0504 寻求帮助

1. 开始

Portal 无感知认证是一种针对智能终端、无须输入用户名和密码即可上线的认证过程。用户第一次使用智能终端时，通过浏览器上网产生流量，设备会重定向到 Portal 认证页面。用户输入用户名、密码、服务等信息后上线，服务器会将认证信息以及终端的 MAC 地址保存到数据库中。当用户再次使用该智能终端访问网络产生流量时，服务器自动使用该认证信息进行认证，免去了用户输入认证信息上线的过程。

Portal 无感知认证排错定位思路：首先检查服务器软硬件及性能是否满足当前认证需要，然后需要确保普通 Portal 网页能正常上线，相应做 iMC 服务器的检查、Portal 无感知相关配置的检查和 RADIUS 相关配置的检查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，可考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，但重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始→智能部署监控代理”命令，选择“部署”标签，检查“用户接入管理”功能模块及“Portal 服务器”功能模块是否已经部署，如图 8-58 所示。



图 8-58　功能模块的部署情况

说明：Potal 无感知认证是基于 EIA 的 Portal 功能的延伸，故必须安装部署 EIA 功能组件及 Portal 服务器。

(2) iMC 服务器运行情况检查

① 打开部署监控代理，查看 uam. exe、portalserver、uamjob 进程是否正常启动。由于 Portal 无感知认证必须是网页 Portal 认证，故必须确认 Portal 服务器上的 jserver/webserver

进程正常启动,如图 8-59 所示。



图 8-59 部署情况

说明:

(a) 一般情况下,这些进程通过鼠标右键设置启动方式为"自动启动"。

(b) jserver 是 Portal 组件集中式部署时所需关注的进程;webserver 为 Portal 组件分布式部署时,在从机上需要确认的进程。

② 检查服务器 1812、1813、50100、50200 UDP 端口是否被 uam 相关进程所监听,如图 8-60 所示。

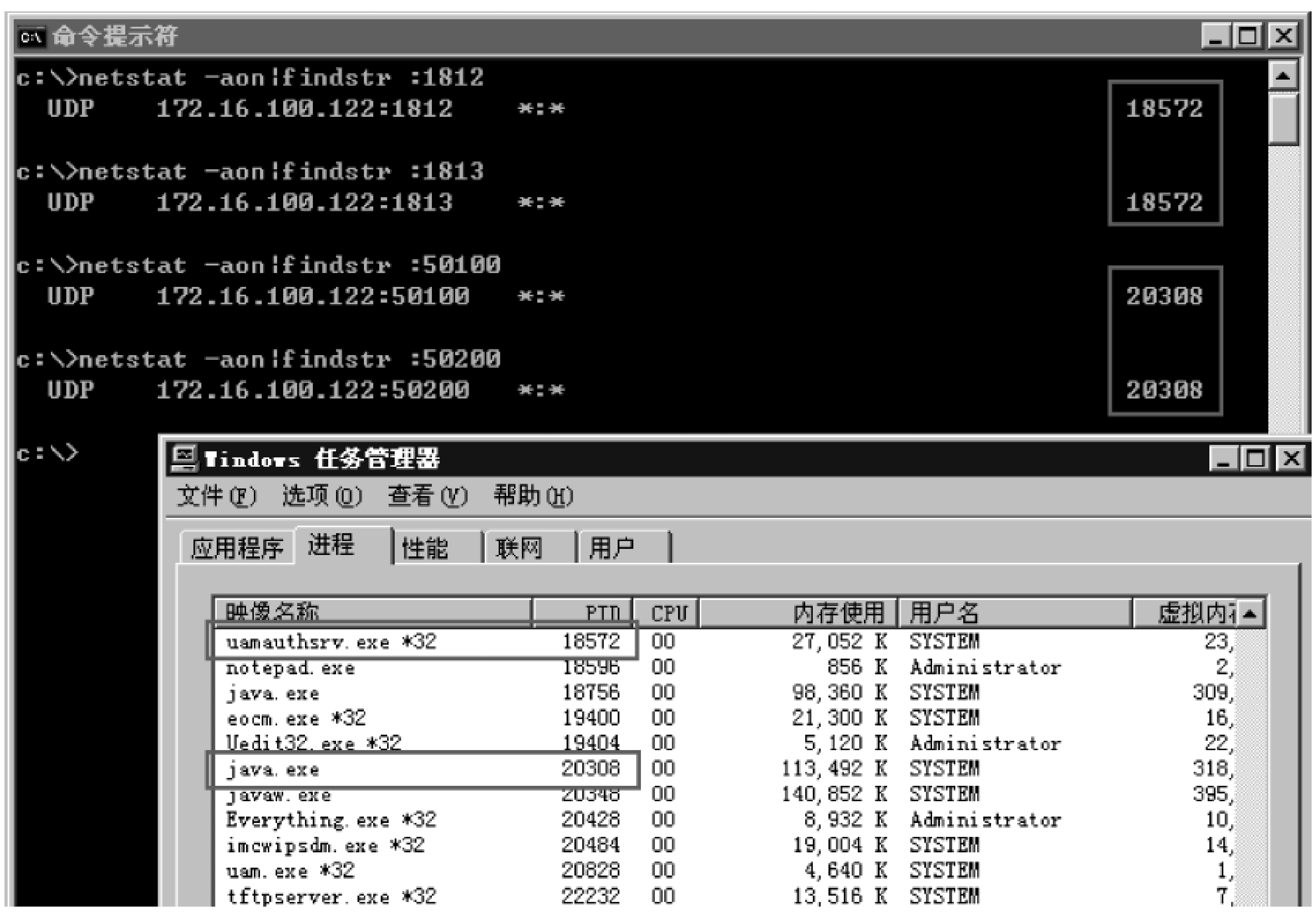


图 8-60 端口被 uam 相关进程监听情况

说明:

(a) Windows 操作系统中,通过

netstat-aon | findstr :端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图8-61所示。

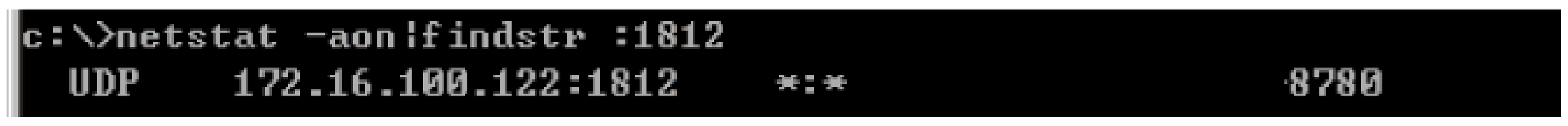


图8-61 命令提示符回显

其中第一列UDP所指监听的协议，第二列10.153.43.100:1812所指监听的服务器的IP和端口号，第三列 *：* 代表此行信息为监听状态，最右一列8780代表此协议监听的进程PID。

(b) 查到端口所对应的进程PID后，请查看Windows任务管理器，1812/1813端口所对应的应为uam相关的进程，50100/50200所对应的为java进程。

(3) iMC服务器和Portal设备、终端可达性检查

Portal认证是对上行流量的认证，并且需要和Portal服务器通信交互Portal报文。对于没有禁ping的环境，在认证上线之前终端PC是可以和Portal所在服务器可达的。分别从iMC服务器上ping接入设备IP、Portal设备IP和终端IP。

(4) 普通Portal网页认证可用性检查

Portal认证Portal在英语中是入口的意思。Portal认证可以使用iNode客户端或Web网页认证，一般将Portal认证网站称为门户网站。基本思想：未认证用户上网时，认证设备会强制用户登录到特定Web站点，用户可以免费访问该Web站点的服务。当用户需要使用互联网中的其他信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。Portal业务可以为客户提供方便的管理功能，门户网站可以开展广告、社区服务等个性化业务，为了方便客户对门户网站的个性化定制。

Portal无感知认证必须基于Web网页认证，基于iNode认证无法实现Portal无感知，故在实施Portal无感知认证前，必须确保普通Portal网页认证正常，再进行Portal无感知的配置。有关普通Portal认证的排查思路，请参考云图《UAM Portal认证排错》。

(5) 设备侧的配置检查

Portal无感知认证是一种基于MAC地址的快速认证的新机制，除了iMC EIA外，还需要接入设备支持，并确保配置正确。

Radius及普通Portal认证命令没有变化，正常配置。Portal无感知认证命令如下。

① 配置MAC绑定服务器信息，并指定Portal服务器及端口号。

<Sysname> system-view

[Sysname] portal mac-trigger server ip 10.153.1.100 port 50111

② 配置MAC认证功能及触发MAC快速认证的阈值。

Interface Vlan3使能Portal并且设置MAC快速认证功能，流量探测周期为300秒，流量触发MAC快速认证的阈值为10KB。

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] portal mac-trigger enable period 300 threshold 10240

(6) Portal服务器侧配置检查

① 接入用户服务检查。请确保EIA中接入用户关联的接入服务都启用了Portal无感知认证功能，即接入服务中要选中“Portal无感知认证”单选框，如图8-62所示。



图 8-62　接入用户服务检查

② Portal 端口组配置检查。检查 EIA 中 Portal 端口组信息中是否启用了 Portal 无感知认证功能，即端口组信息中“无感知认证”选项为“支持”，如图 8-63 所示。



图 8-63　Portal 端口组配置检查

③ EIA 中的 HTTP 特征库列表检查 EIA 中的 HTTP 特征库列表检查，如图 8-64 所示。



图 8-64　EIA 中的 HTTP 特征库列表检查

说明：只有与 EIA 中 HTTP 特性相匹配的终端才允许进行 Portal 无感知认证，EIA V7 版本默认仅支持智能终端特征库，如果需要支持其他终端类型，可以按需增加。

HTTP 特征来自于终端浏览器的 HTTP 报文中的“User-Agent”字段内容，可以通过抓包工具解析，如图 8-65 所示。

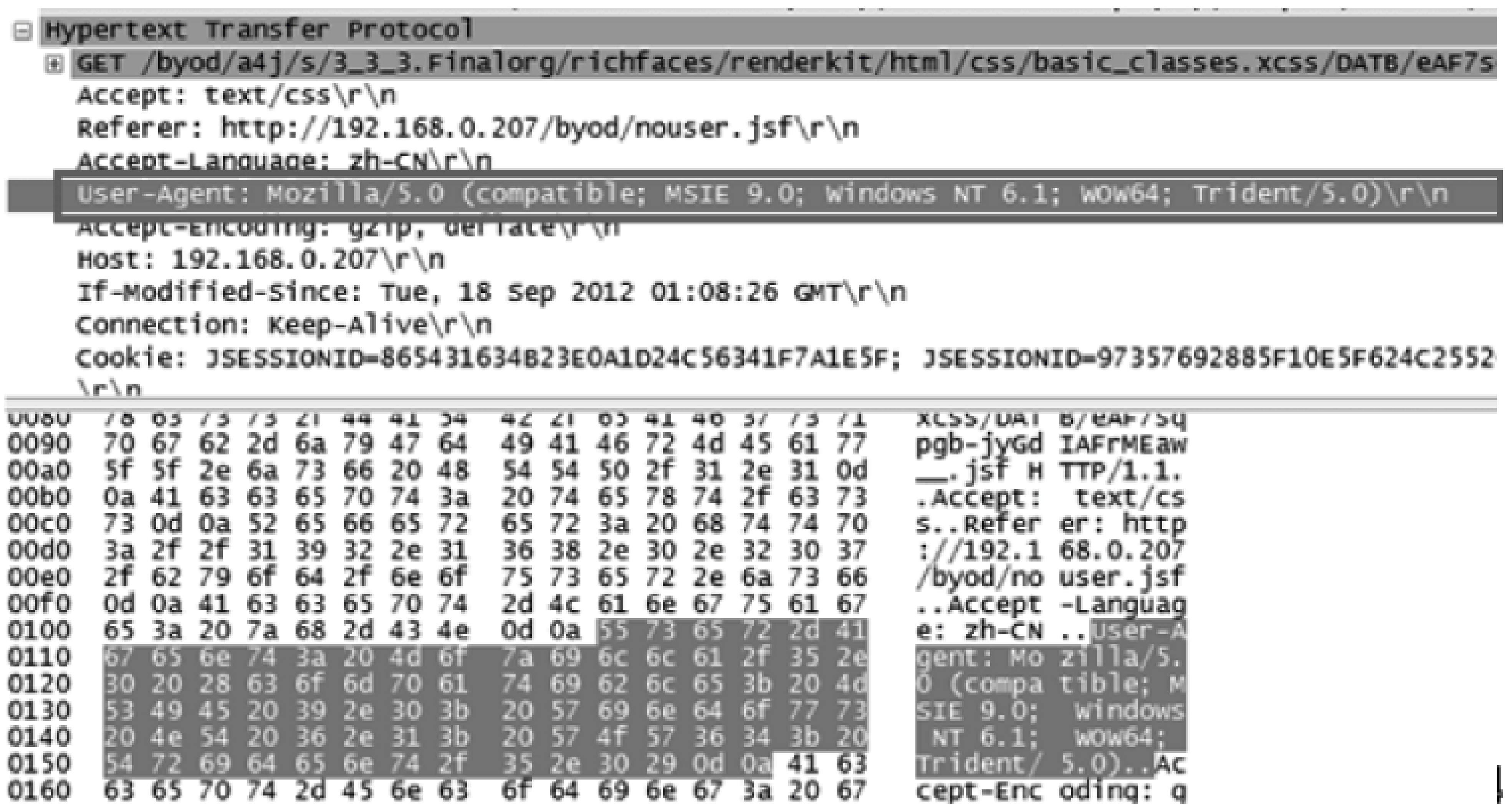


图 8-65　抓包工具解析

然后在 EIA 侧增加相应的 HTTP 特征，如图 8-66 所示。

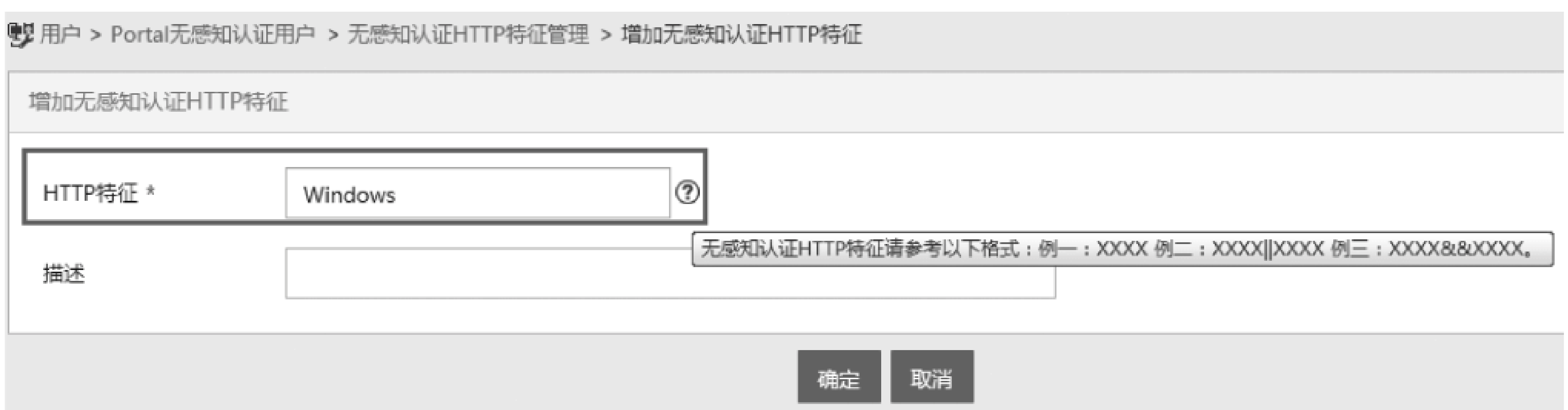


图 8-66　EIA 侧增加相应 HTTP 特征

如果所有终端都要实现 Portal 无感知认证，则只要增加一条 HTTP 特征为“All”的记录即可，如图 8-67 所示。



图 8-67　增加“All”记录

④ 终端 MAC 地址绑定检查。Portal 无感知认证强依赖于终端的 MAC 地址，故 Portal 无感知认证的最基本要求是认证设备必须通过 Radius 协议的 Access-Request 报文上传终端的 MAC 地址给 EIA 服务器，才能完成账号和 MAC 地址的绑定操作，Portal 无感知才会成功生效。有关终端 MAC 地址绑定失败的可能性如下。

(a) 设备未上传终端的 MAC 地址。请检查现场组网是否为二层 Portal，即 Portal 认证设

备是否是终端的网关设备。三层 Portal 场景设备无法上传终端 MAC 地址，在 EIA 服务器侧抓包查看 Radius 协议的 Access-Request 报文的 Calling-Station-id 属性值为：0000-00000-00000，如图 8-68 所示。

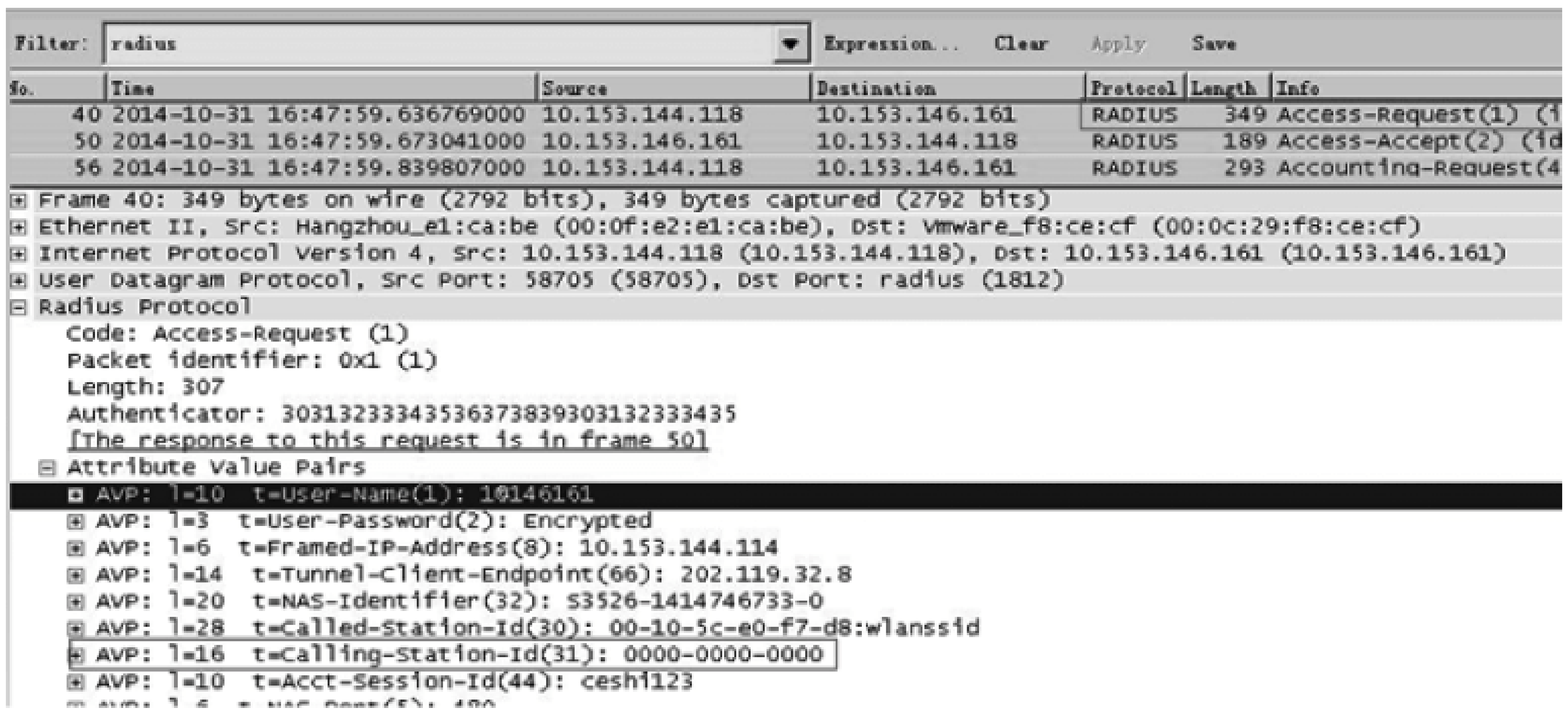
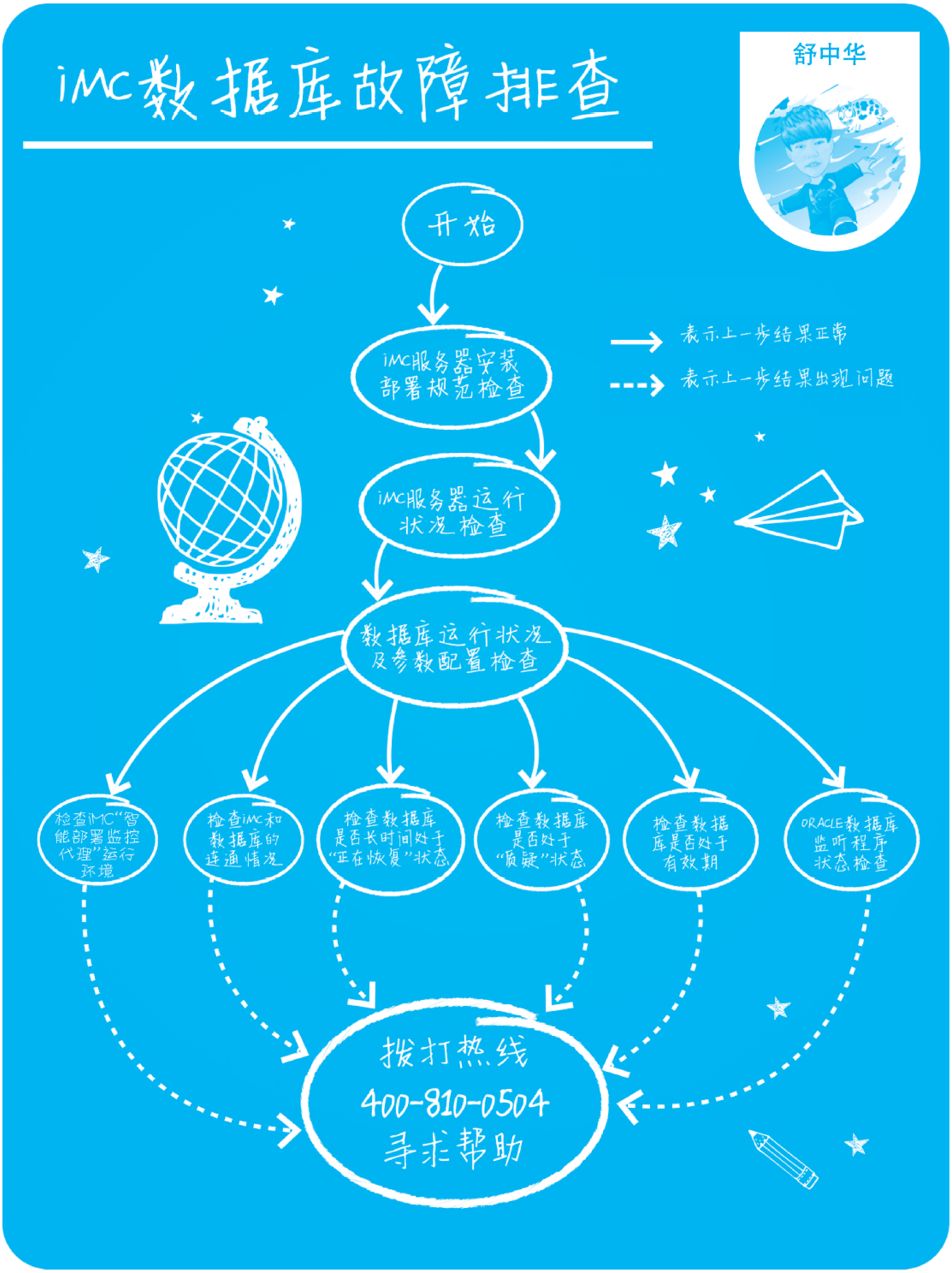


图 8-68　增加无感知认证 HTTP 特征

（b）设备上传了终端 MAC 地址，但账号和 MAC 地址绑定失败。请检查绑定的 MAC 地址数是否超出了用户设置的 Portal 无感知认证最大绑定数。请在接入用户信息中查看 Portal 无感知认证 MAC 地址绑定信息及账号 Portal 无感知最大绑定数如图 8-69 所示。



图 8-69　接入用户信息



iMC数据库故障排查
舒中华
开始
iMC服务器安装部署规范检查
iMC服务器运行状况检查
数据库运行状况及参数配置检查
表示上一步结果正常
表示上一步结果出现问题
检查iMC“智能部署监控代理”运行环境
检查iMC和数据库的连通情况
检查数据库是否长时间处于“正在恢复”状态
检查数据库是否处于“质疑”状态
检查数据库是否处于有效期
ORACLE数据库监听程序状态检查
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC 强依赖后台数据库，iMC 后台所有数据都存放在数据库表项中，包括 SQL 和 Oracle，数据库程序异常，会直接影响 iMC 的正常运行及数据的完整性。在 iMC 的日常维护过程中，有很多由于数据库异常而导致 iMC 不可用的经验案例。

iMC 数据库故障的定位思路：首先检查服务器软硬件及性能是否满足当前需要，然后检查 iMC 相应进程运行及数据库连接是否正常，最后检查数据库的运行情况，包括数据库服务、连接参数、是否在有效期内等。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是推荐的运行 iMC 最基本的部署要求，请严格执行。

对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，是否需要分布式部署。重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

(2) iMC 服务器运行状况检查

① 检查服务器当前操作系统版本是否满足 iMC 安装要求。

② 检查当前操作系统是否是正版。

③ 检查服务器内存、CPU 使用百分比是否正常。

(3) 数据库运行状况及参数配置检查

① 检查数据库服务是否运行正常

以 SQL Server 2008 R2 举例。

单击“开始菜单”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在弹出如图 8-70 所示对话框中，检查各服务的状态是否“正在运行”。

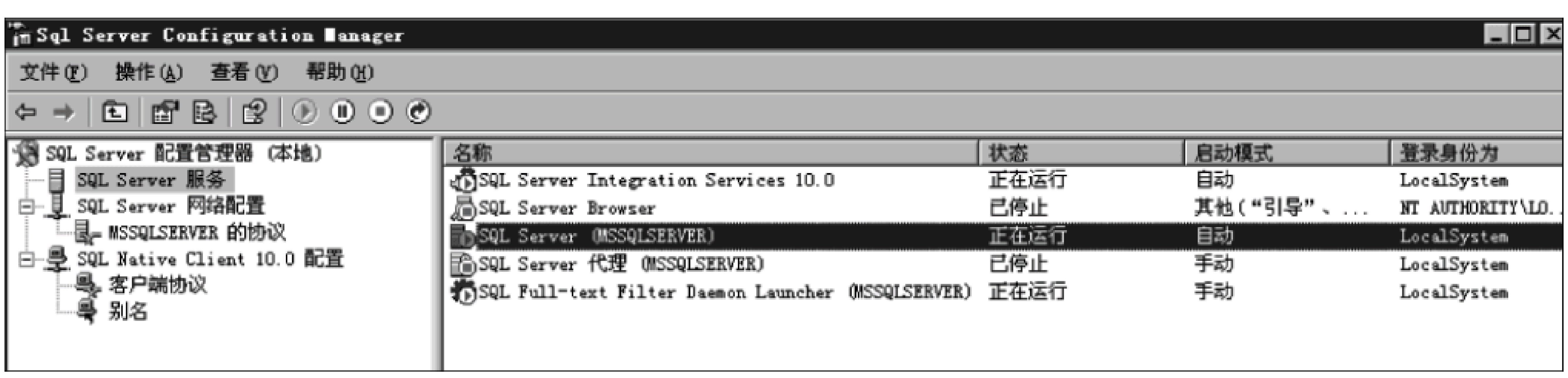


图 8-70 检查数据库服务是否运行正常

说明：

(a) SQL Server(MSSQLSERVER)是 SQL 的最主要服务，必须处于“正在运行”状态。

(b) iMC 要求 SQL Server(MSSQLSERVER)服务必须以 LocalSystem 身份登录。

② 检查数据库的相关参数配置是否正确

(a) TCP/IP 参数检查

以 SQL Server 2008 R2 举例。

单击“开始菜单”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在弹出如图 8-71 所示对话框中，选中左侧树上的“SQL Server 网络配置→MSSQLSERVER 的协议”，在右侧界面中，双击“TCP/IP”打开“TCP/IP 属性”配置对话框。



图 8-71 “Sql Server Configuration Manager”对话框

在“协议”标签中确认“全部侦听”为“是”，如图 8-72 所示。

在“IP 地址”标签下，确认各个 IP 地址下的“已启用”为“是”，“TCP 端口(TCP Port)”为“1433”，如图 8-73 所示。

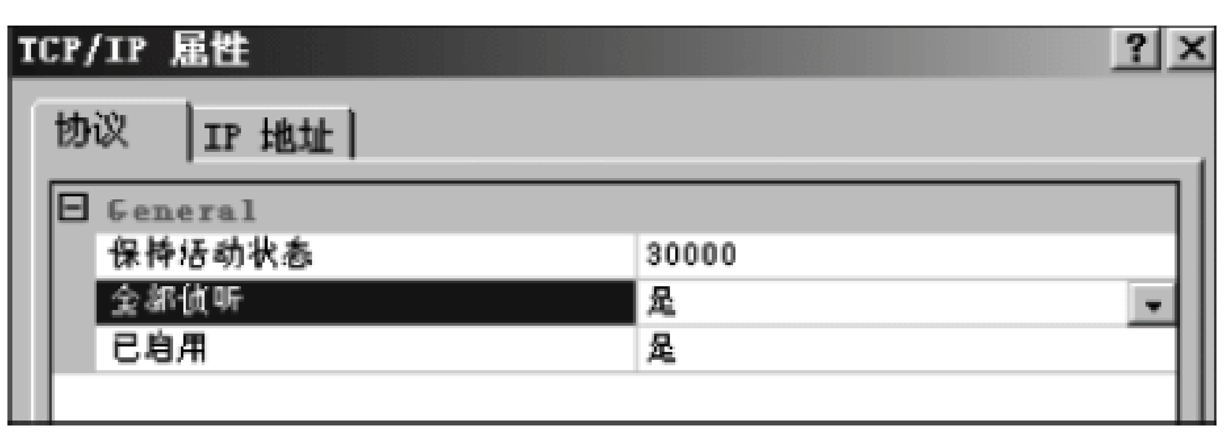


图 8-72 “协议”标签

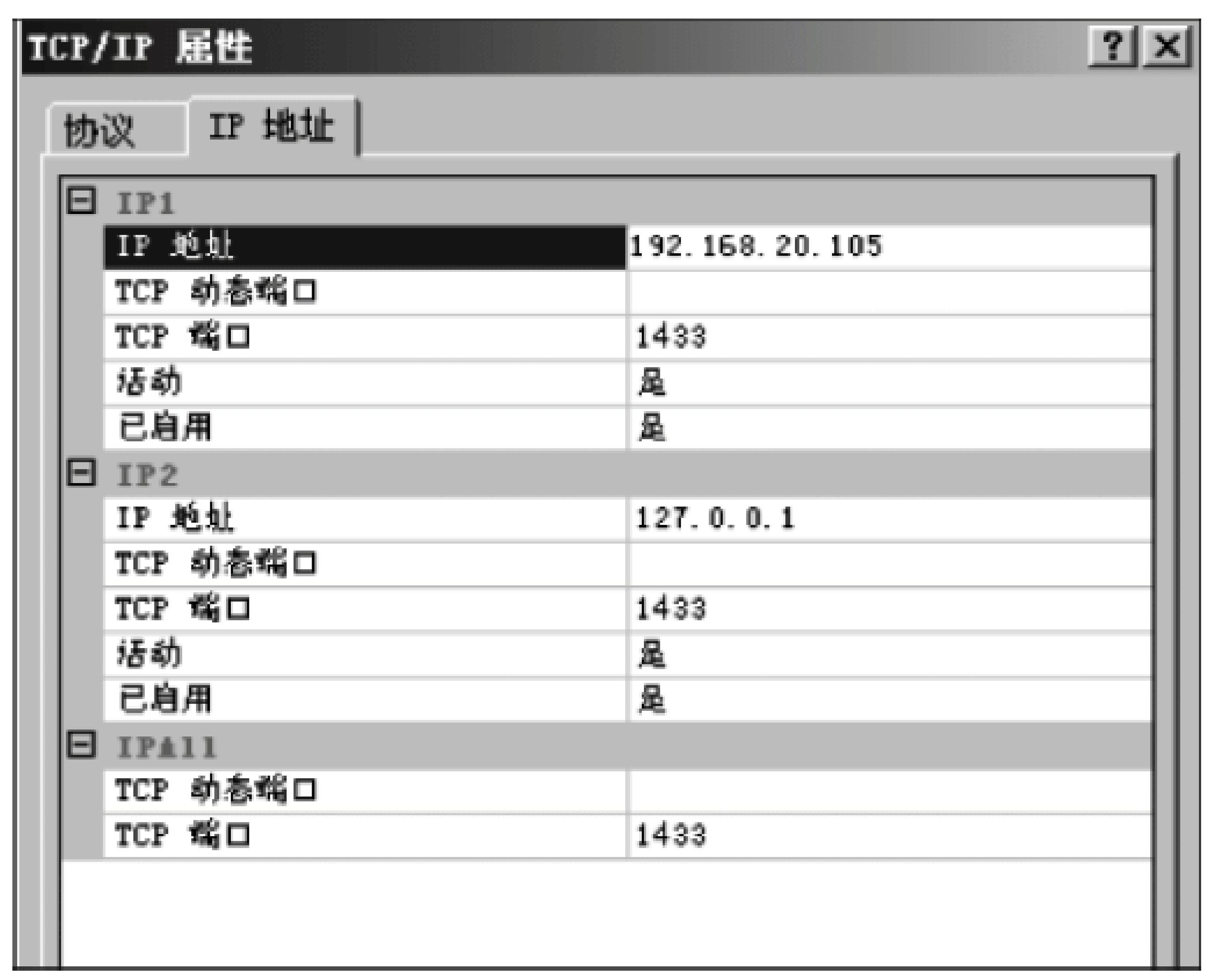


图 8-73 “IP 地址”标签

说明：

ⓐ 如果前面“TCP/IP 属性”配置界面中，没有将“全部侦听(Listen All)”的值改为“是(Yes)”，则在 SQL Server 2008 R2 安装完成后，如果服务器的 IP 地址更改了，必须重新进入该配置窗口，将原来配置的“IP 地址(IP Address)”进行更新，否则无法连接数据库。

ⓑ 同样方法确认 Named Pipes 属性也被使能。

ⓒ 在分布式部署场景中，如果使用了多个数据库服务器，各服务器的监听端口必须相同。

(b) 检查 SQL Server 的登录方式

单击“开始菜单”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在如图 8-74 所示对话框中查看 SQL Server 服务的“登录身份为”

列，确保其值为“LocalSystem”。

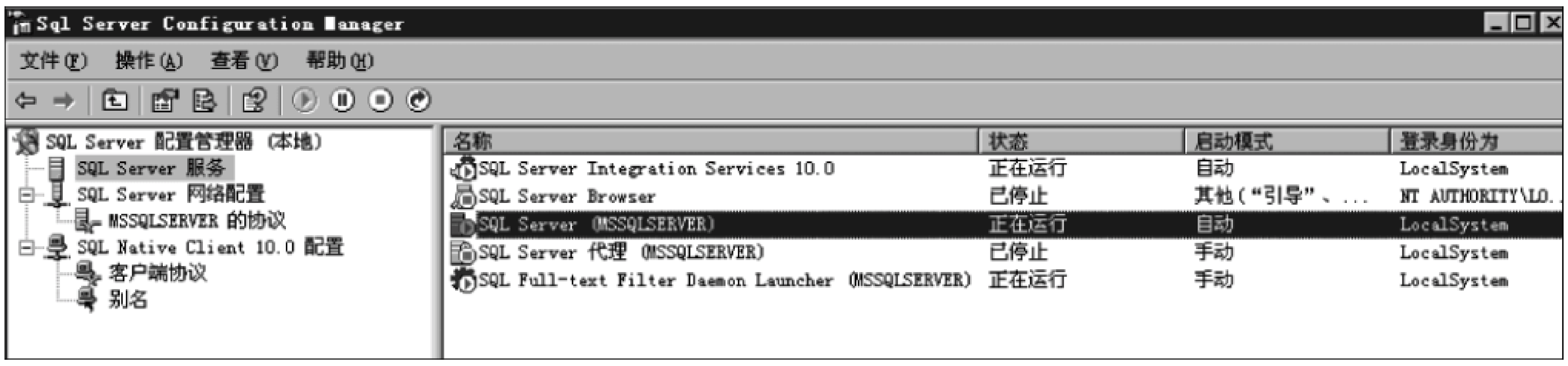


图 8-74　检查 SQL Server 的登录方式

如果当前不是“LocalSystem”身份登录，需要将其改为“Local System”。双击该行（或选中该行后，单击工具栏中的“属性”按钮），打开“SQL Server 属性”配置对话框，如图 8-75 所示，将“登录身份为”改为“内置账户”中的“本地系统（LocalSystem）”。



图 8-75　“SQL Server 属性”配置对话框

③ 检查当前数据库版本是否存在已知 BUG

在 KMS 系统中搜索经验案例及技术公告，排查当前数据库版本是否存在已知 BUG，例如：之前在某局点碰到过由于 SQL 已知 BUG 导致 iMC 异常的案例，产品线已输出技术公告并归档 KMS《关于 SQL Server 2008 R2 存在 Default 内存不足而影响 iMC 正常运行的公告》。

（4）检查 iMC“智能部署监控代理”运行环境

单击“开始”→“智能部署监控代理”命令，选择“运行环境”标签，正常情况如图 8-76 所示，能正常显示数据库空间使用情况。

异常情况下，查看“智能部署监控代理”的“运行环境”标签会出现“数据库连接失败，请检查数据库是否可用”的提示，如图 8-77 所示。

（5）检查 iMC 和数据库的连通情况

SQL Server 客户端 SQL Management Studio 安装完成后，请参照以下步骤测试与 SQL Server 服务器的连接状况，确认客户端和服务器是否能够正常连接。

① 单击系统“开始”→“运行”命令，在运行窗口中输入 cmd，进入命令行模式。

② 输入以下命令。

osql -S172.8.9.63 -Usa -PiMC123

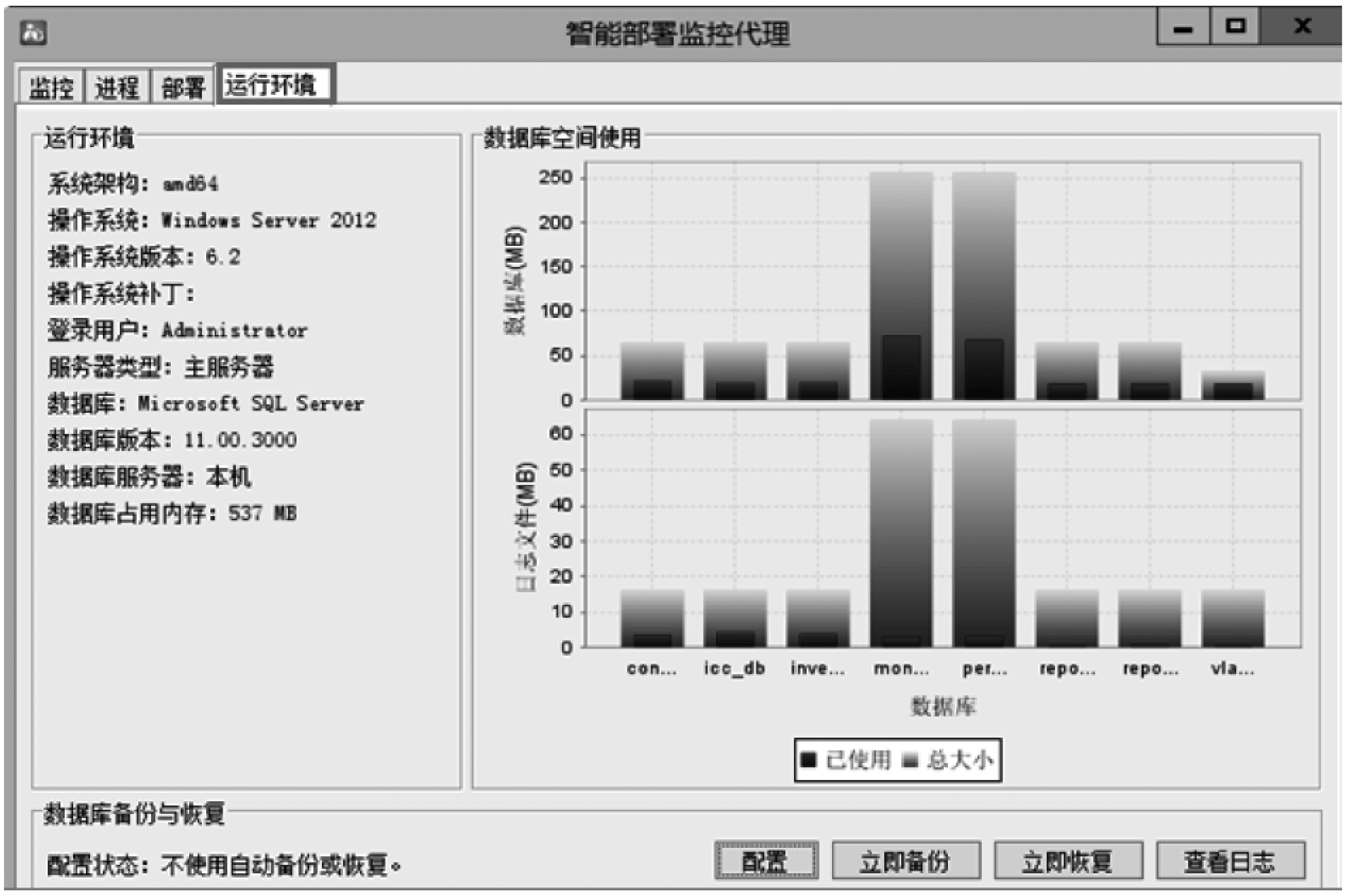


图 8-76　正常情况下“运行环境”标签



图 8-77　异常情况下“运行环境”标签

其中 172.8.9.63 为 SQL Server 服务器 IP 地址，sa 为默认超级用户，iMC123 为 sa 用户的密码。如果 SQL Server 服务器没有使用默认实例名，还需要在命令中指定实例名称，命令如下。

osql -S172.8.9.63\instancename -Usa -PiMC123//instancename 为实例名称。

③ 如果能够进入 SQL 命令模式，则表明能正常连接到服务器，如图 8-78 所示。

(6) 检查数据库是否长时间处于“正在恢复”状态

在 iMC 智能部署监控代理中去部署组件时，会提示是否删除数据库。有时候处理不当，

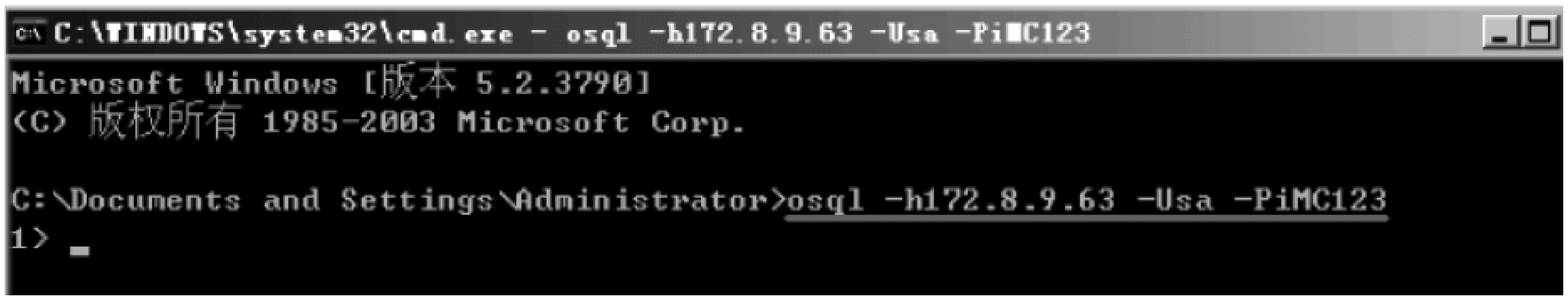


图 8-78　SQL 命令模式

数据库会删除不彻底，再安装该组件时 iMC 会报错。登录 SQL Server Management Studio 查看，该组件的数据库会处于“正在恢复”的状态。影响业务组件的继续部署。登录 SQL Server Management Studio，也无法手工删除该数据库时，可用使用如下 SQL 脚本进行数据库恢复。

--DataBaseName 为修复的数据名，如 syslog_db。

```
USE MASTER
GO
SP_CONFIGURE 'ALLOW UPDATES',1 RECONFIGURE WITH OVERRIDE
GO
ALTER DATABASE [DataBaseName] SET EMERGENCY
GO
sp_dboption 'DataBaseName', 'single user', 'true'GO
DBCC CHECKDB('DataBaseName','REPAIR_ALLOW_DATA_LOSS')
GO
ALTER DATABASE [DataBaseName] SET ONLINE
GO
sp_configure 'allow updates', 0 reconfigure with override
GO
sp_dboption 'DataBaseName', 'single user', 'false'GO
```

说明：执行如上 SQL 脚本存在数据丢失的风险，操作前一定要知会客户所存在的风险，建议客户寻找专业的数据库厂商处理。

（7）检查数据库是否处于“质疑”状态

访问 iMC 的 Web 页面提示连接不上 ** 数据库，打开部署监控代理“进程”查看对应的进程提示“进程启动未知错误”，以 UBA 组件为例，提示 unbaserver 进程启动未知错误，如图 8-79 所示。

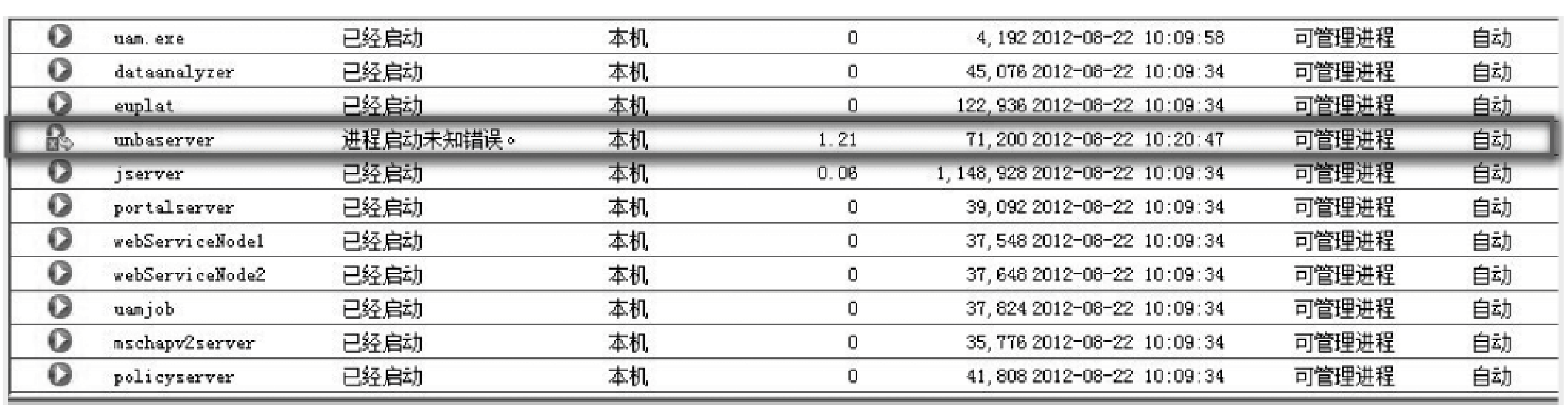


图 8-79　unbaserver 进程启动未知错误

在“智能部署监控代理”的“运行环境”标签中会提示“数据库连接失败，请检查数据库是否可用”，如图 8-80 所示。

单击“配置”按钮，弹出的对话框会提示连接不上哪些数据库，具体如图 8-81 所示，对话框中会列出异常的数据库名称。

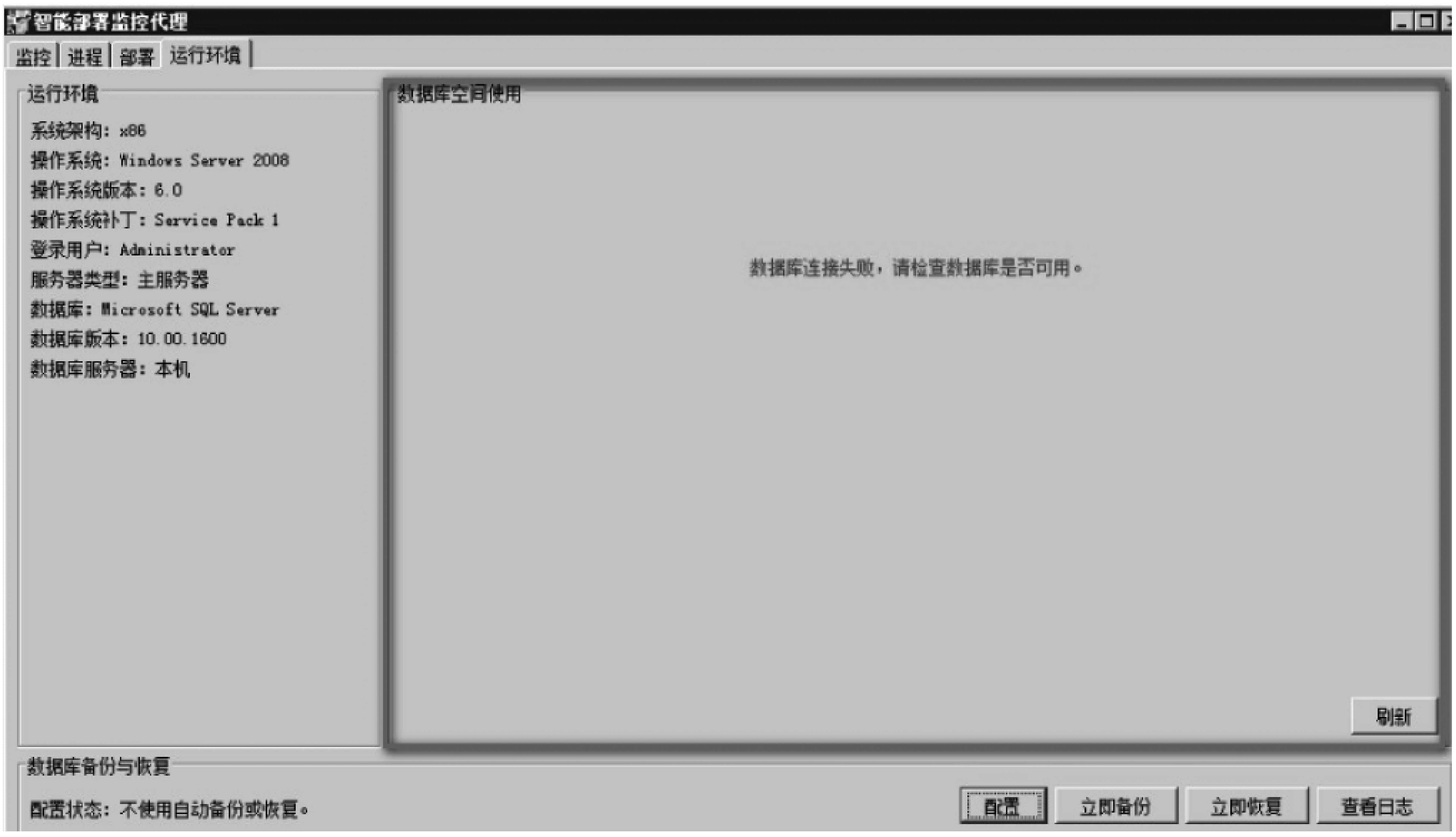


图 8-80 “运行环境”标签中的提示



图 8-81 异常数据库名称

此时，通过 SQL 客户端 SQL Server Managment Studio 登录到 SQL 发现对应的数据库被质疑，英文版 SQL 的数据库会被标示 Suspect 字样，具体如图 8-82 所示。

该问题经常发生在由于硬盘空间不够或硬盘读写错误，异常关机等原因导致 SQL 数据库被质疑，解决方法如下。

打开数据库里的 SQL 查询编辑器窗口，分别执行如图 8-83 所示的命令。

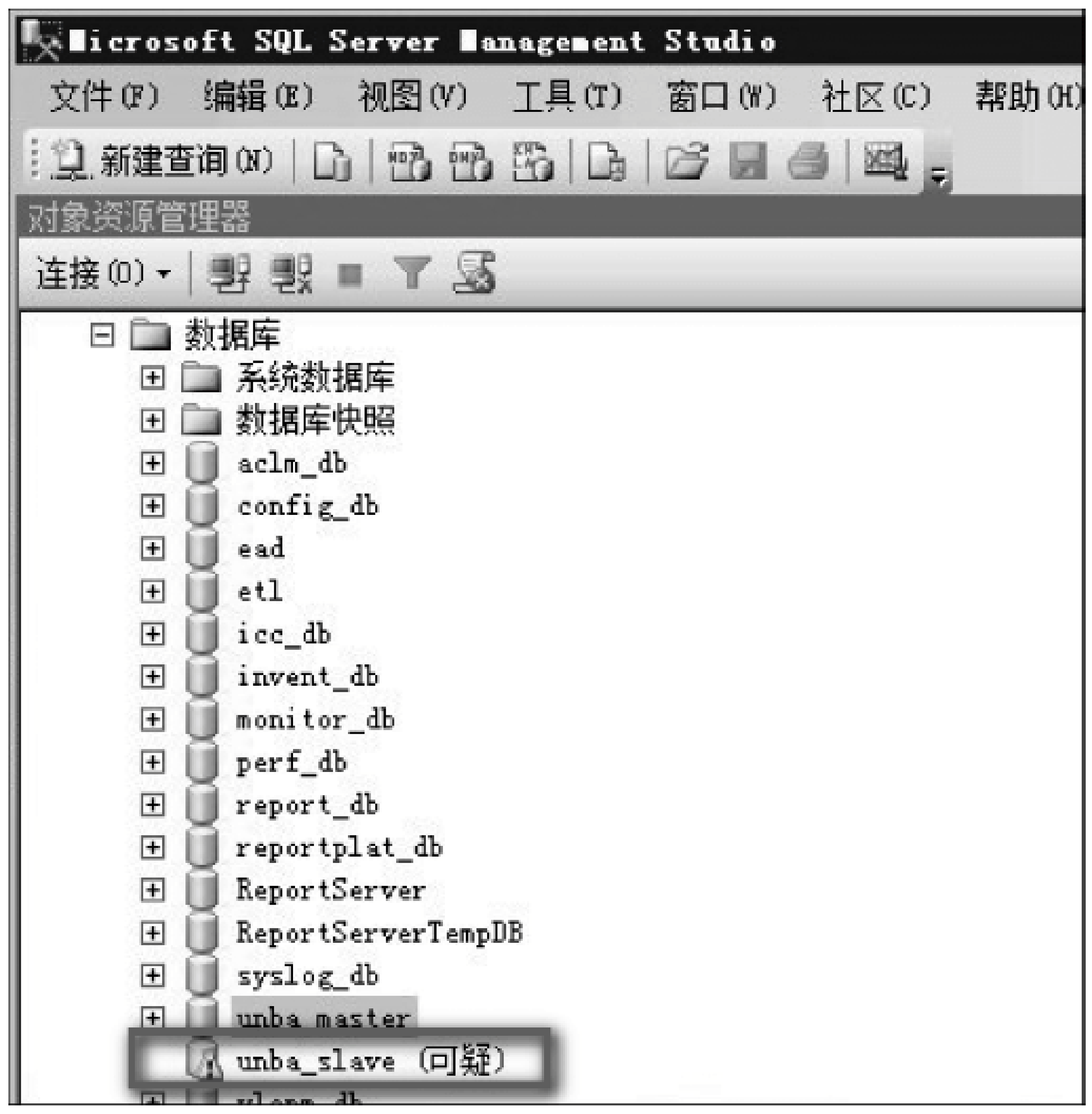


图 8-82 数据库被质疑

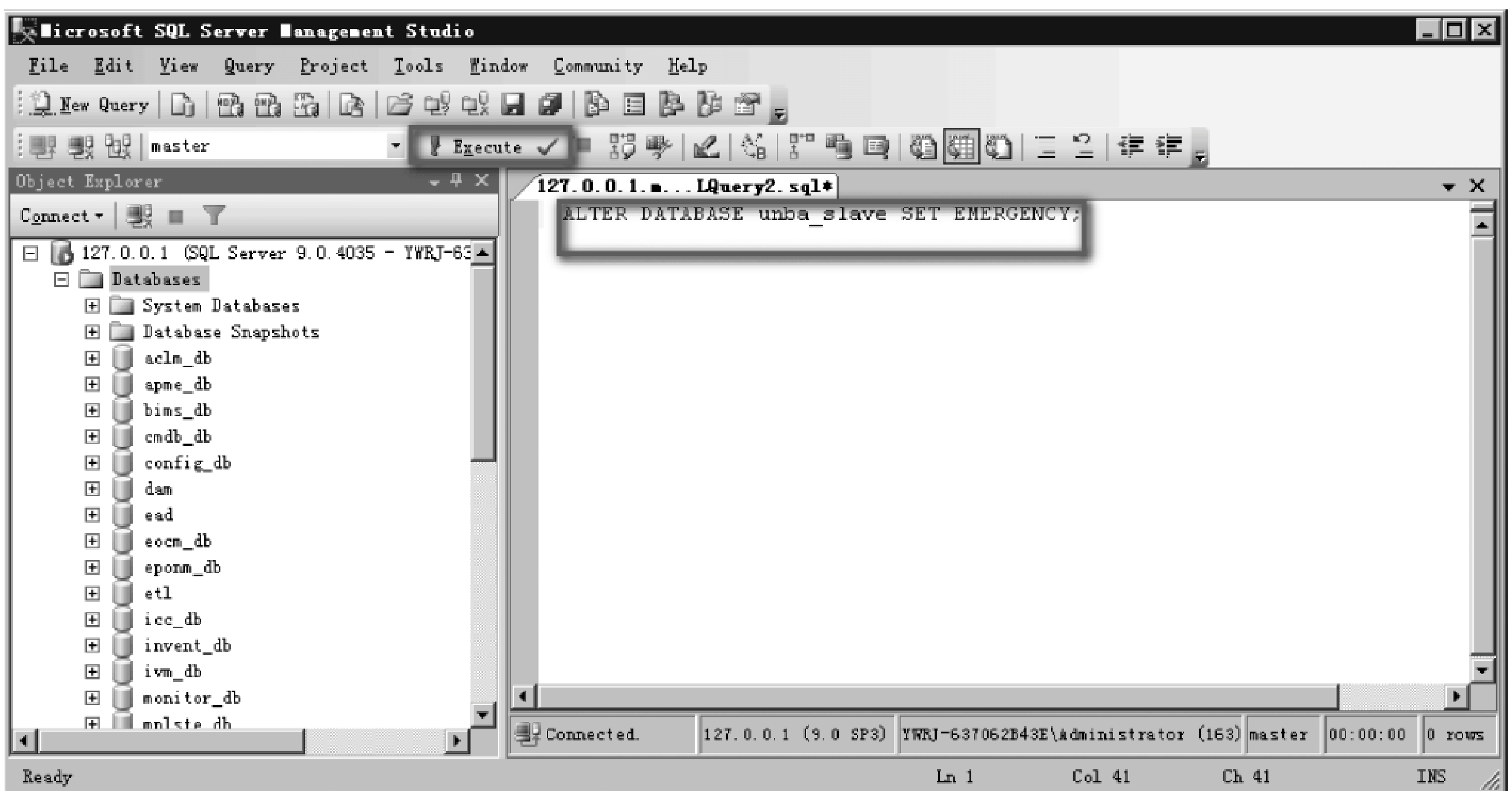


图 8-83 在 SQL 查询编辑窗口中执行命令

① 修改数据库为紧急模式。

ALTER DATABASE unba_slave SET EMERGENCY。

② 使数据库变为单用户模式。

ALTER DATABASE unba_slave SET SINGLE_USER。

③ 修复数据库日志重新生成,此命令检查的分配,结构,逻辑完整性和所有数据库中的对象错误。当指定“REPAIR_ALLOW_DATA_LOSS”作为 DBCC CheckDB 命令参数,该程序将检查和修复报告的错误。但是,这些修复可能会导致一些数据丢失。

DBCC CheckDB (unba_slave, REPAIR_ALLOW_DATA_LOSS)

④ 使数据库变回为多用户模式。

ALTER DATABASE unba_slave SET MULTI_USER。

⑤ 重启 SQL 进程,使用 SQL Server Managment Studio 登录数据库查看对应的进程是否正常。

说明:

(a) 如果数据量比较大,这里需要注意一下,自动恢复时 tempdb 数据库会随着修复而占用磁盘空间,默认的 tempdb 是在系统盘,如果系统盘不够大,就会修复失败,这时可以考虑将 tempdb 数据库转移到磁盘空间较大的磁盘里。

(b) 执行如上 SQL 脚本存在数据丢失的风险,操作前一定要知会客户所存在的风险,建议客户寻找专业的数据库厂商处理。

(8) 检查数据库是否处于有效期

检查数据库是否正版,部分局点使用的 SQL Server 为评估版本,一旦过了试用期 180 天后,SQL Server 服务不能正常启动。手工启动服务会有如下提示,错误代码:17051,如图 8-84 所示。



图 8-84 手工启动服务提示

解决方案是使用正版密钥安装正式发布版本。

(9) Oracle 数据库监听程序状态检查

Oracle 监听器 Listener 是一个重要的数据库服务器组件,在整个 Oracle 体系结构中,扮演着重要的作用,总结监听程序(Listener)的功能如下。

① 监听客户端请求。监听器运行在数据库服务器之上,与 Oracle 实例(可为多个)相关联,是一个专门的进程(Process),在 Windows 的服务项目或 Linux 的运行进程列表中,都会看到对应的运行进程。Windows 上名为 TNSLSNR,Linux/UNIX 平台上是 Lsnrctl。监听器守候在服务器制定端口(默认为 1521),监听客户端的请求。

② 为客户端请求分配 Server Process。监听器只负责接听请求,之后将请求转接给 Oracle Server Process。在 Oracle 的服务模式下,客户端进程是不允许直接操作数据库实例和数据,而是通过一个服务进程 Server Process(也称为影子进程)作为代理。监听器接收到请求之后,就向操作系统(或者 Dispatcher 组件)要求 fork(或分配)一个 Server Process 与客户端相连。

③ 注册实例服务。本质上讲,Listener 是建立实例和客户端进程之间联系的桥梁。Listener 与实例之间的联系就是通过注册的过程来实现的。注册的过程就是实例告诉监听器,它的数据库实例名称 instance_name 和服务名 service_names。监听器注册上这样的信息,对客户端请求根据监听注册信息,找到正确的服务实例名称。目前 Oracle 版本中,提供动态注册和静态注册两种方式。

④ 错误转移 Failover。Failover 是 RAC 容错的一个重要方面的功能,其功能是在数据库实例崩溃的时候,可以自动将请求转移到其他可用实例上的一种功能。可以提供很大程度上

的可用性(Availability)功能。这个过程中,发现实例已经崩溃,并且将请求转移到其他实例上,就属于是 Listener 的功能。

⑤ 负载均衡衡量。在 RAC 架构中,Oracle 实现了负载均衡。当一个客户请求到来时,Oracle 会根据当前 RAC 集群环境中所有实例的负载情况,避开负载较高的实例,将请求转移到负载较低的实例中进行处理。在早期 RAC 版本中,负载轻重的衡量是根据监听器当前维护连接数目来确定的,而不是实时查看多实例的负载。RAC 环境中的监听器之间进行沟通通信。一旦监听程序工作异常,其他应用程序将无法正常访问 Oracle 数据库,Oracle 监听程序的运行状态排查方法如下。

(a) 使用命令:lnsrctl service 查看监听程序的状态

```
[root ~]# lsnrctl service
LSNRCTL for Linux: Version 11.2.0.2.0 - Production on 22-NOV-2012 13:52:11
Copyright (c) 1991, 2010, Oracle.   All rights reserved.
Connecting to (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521))
TNS-12541: TNS:no listener
TNS-12560: TNS:protocol adapter error
TNS-00511: No listener
Linux Error: 111: Connection refused
```

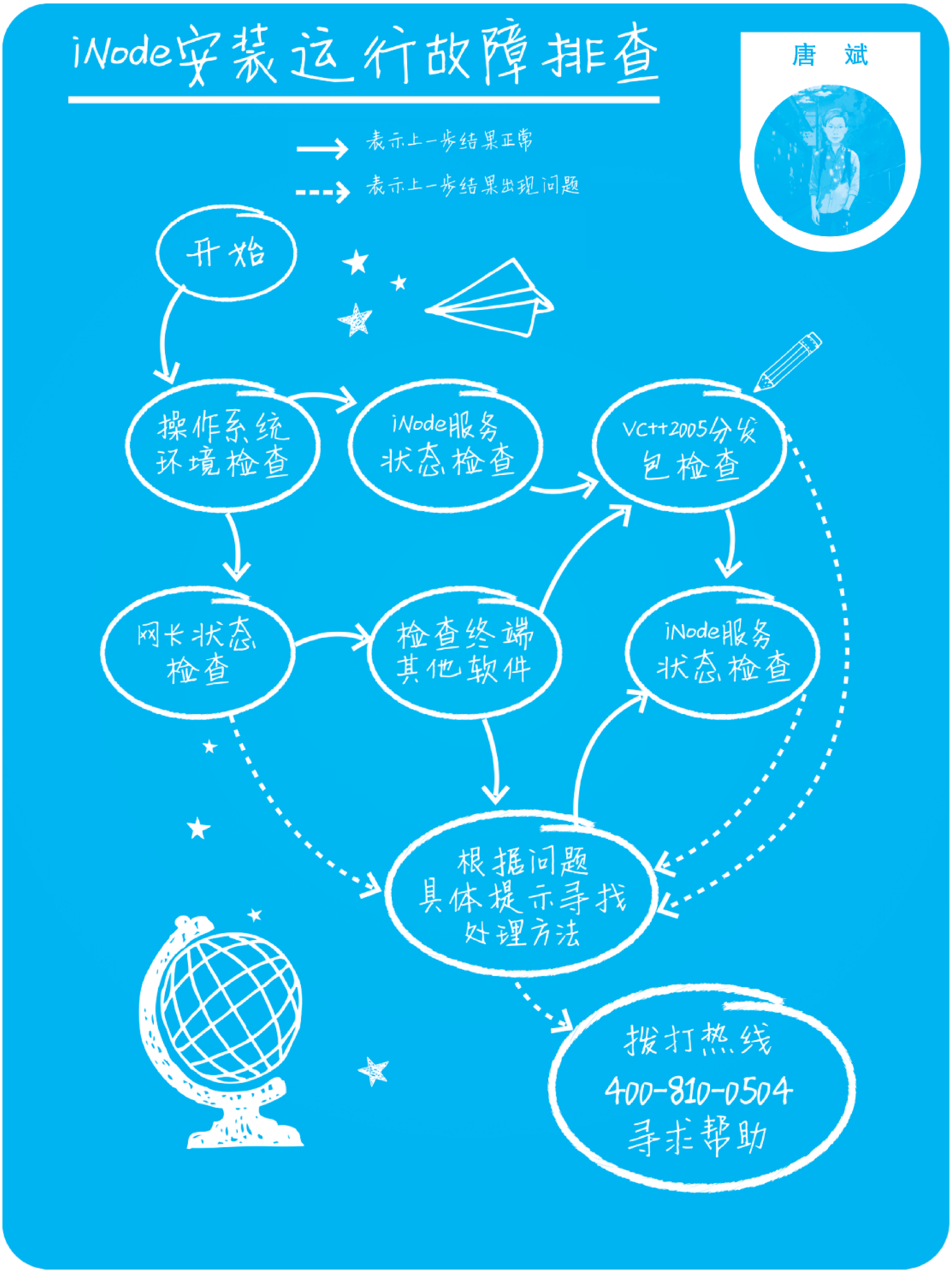
(b) 查看监听程序日志大小

```
[root]# cd /opt/app/oracle/product/10.2.0/db/network/log
[root@nicrac log]# du -shlistenner.log
2.1G      listenner.log
```

由于 32 位 Linux 系统环境下,监听程序日志文件(listenner.log)不能超过 2GB,当该文件累计超出 2GB 限制后,将影响监听程序的正常启动。解决方法是将该日志文件清空,操作方法如下。

```
cd/u01/app/oracle/product/10.2.0/db/network/log/
cat /dev/null>listener.log
```

然后使用命令 lsnrctl start 重启监听程序即可。


iNode安装运行故障排查
唐 斌
表示上一步结果正常
表示上一步结果出现问题
开始
操作系统环境检查
iNode服务状态检查
VC++2005分发包检查
网卡状态检查
检查终端其他软件
iNode服务状态检查
根据问题具体提示寻找处理方法
拨打热线
400-810-0504
寻求帮助

1. 开始

故障定位思路：iNode 作为一款客户端软件，适配在各种操作系统版本上运行。在 iNode 的安装与运行过程中，需要调配操作系统资源，调用操作系统 API 接口。大部分情况，系统环境还存在各种第三方软件和插件。因此，在个别终端上 iNode 安装或运行中遇到问题，可以从操作系统环境不满足条件的角度入手。如检查系统用户权限、查看网卡驱动、排查防控软件等。

2. 流程图相关操作说明

(1) 操作系统环境检查

操作系统功能完整，系统用户权限足够，是保证 iNode 安装运行正常的基本要素。因此在安装前，或安装运行中出现问题故障时，首先需要确认操作系统的基本环境是否符合要求。

① iNode 版本说明书中对 iNode 的运行环境如下，请根据 iNode 版本信息，查找对应的版本说明书。请注意早期版本 iNode 不支持最新的 Windows 操作系统。

② 要求以操作系统管理员权限安装或运行 iNode。

③ 不能在中文路径下安装。检查安装 iNode 的文件夹权限是否正常，如安装路径 C:\是否有写的权限。

说明：举例 iNode 7.1 E0305 的版本说明书如表 8-1 所示。

表 8-1　iNode 7.1 E0305 版本说明书

操作系统	硬件要求	浏览器配置要求
• Windows XP(需要安装 SP2 或以上补丁) • Windows Server 2003(需要安装 SP2 或以上补丁) • Windows Vista(需要安装 SP1 或以上补丁) • Windows 7 Home Basic(家庭基础版) • Windows 7 Home Premium(家庭高级版) • Windows 7 Professional(专业版) • Windows 7 Enterprise(企业版) • Windows 7 Ultimate(旗舰版) • Windows 8 Professional(专业版) • Windows 8 Enterprise(企业版) • Windows 8.1 Professional(专业版) • Windows 8.1 Enterprise(企业版)	主频 1.5GHz(以上) 内存 512MB(以上) 硬盘 20GB(以上) 100Mbps 网卡(以上)	IE 6.0 SP1 及以上版本 Firefox 3.0 及以上版本

说明：

(a) 操作系统用户权限查看方法。用管理员权限打开 CMD，通过命令"net user"查看当前计算机用户的所有系统用户。使用"net user 用户名"查询具体用户的信息，关注该用户是否有管理员权限。若没有权限，建议更换用户登录，或请终端管理员帮助添加权限，如图 8-85 所示。



图 8-85 操作系统用户权限查看方法

(b) 文件夹权限添加方法。打开我的电脑，在菜单栏中单击“工具”→“文件夹选项”→“查看”→“使用简单文件共享”命令取消选中。需要设置写入权限的文件夹上单击“右键”→“属性”→“安全”→“添加”→“Everyone”→“选择的相应的控制权限”命令。具体相关自行查找 Windows 相关资料。

(2) 网卡状态网络协议检查

iNode 作为一款进行拨号上线的客户端软件，网卡的状态或网卡驱动的工作情况非常影响 iNode 的正常工作。正常的网卡应该正常获取 IP，不会显示故障状态，查询网卡信息不会报驱动错误。

① 通过单击“开始”→“运行”→“ipconfig /all”命令查看网卡信息。在没有认证的环境下显示的网卡 IP、网关、DNS 是否正常。使用 arp -a 的命令查看获取网关的 mac 信息等。检查 ping 本地 IP 是否正常。使用 route print 查看终端的路由表，检查路由情况。

② 在系统“设备管理器”中查看网卡状态，如图 8-86、图 8-87 所示。

说明： 若 iNode 有定制客户端 ACL 和防内网外联功能，网卡下会存在 iNode 的驱动，如图 8-88 所示。

③ 单击“网络和共享中心”，在“本地连接”里单击“属性”按钮。可以查看当前连接里的相关网络协议是否正常，如图 8-89 所示。

说明： 网卡故障的情况下，建议先对网卡驱动进行升级或重装。

(3) 安装包文件检查

iNode 安装运行出现问题，也有可能是安装包不完整。建议下载或传输安装文件时，最好将安装文件做成压缩包。完整性可以通过对比文件大小，或者使用 MD5 校验安装包的完整性。

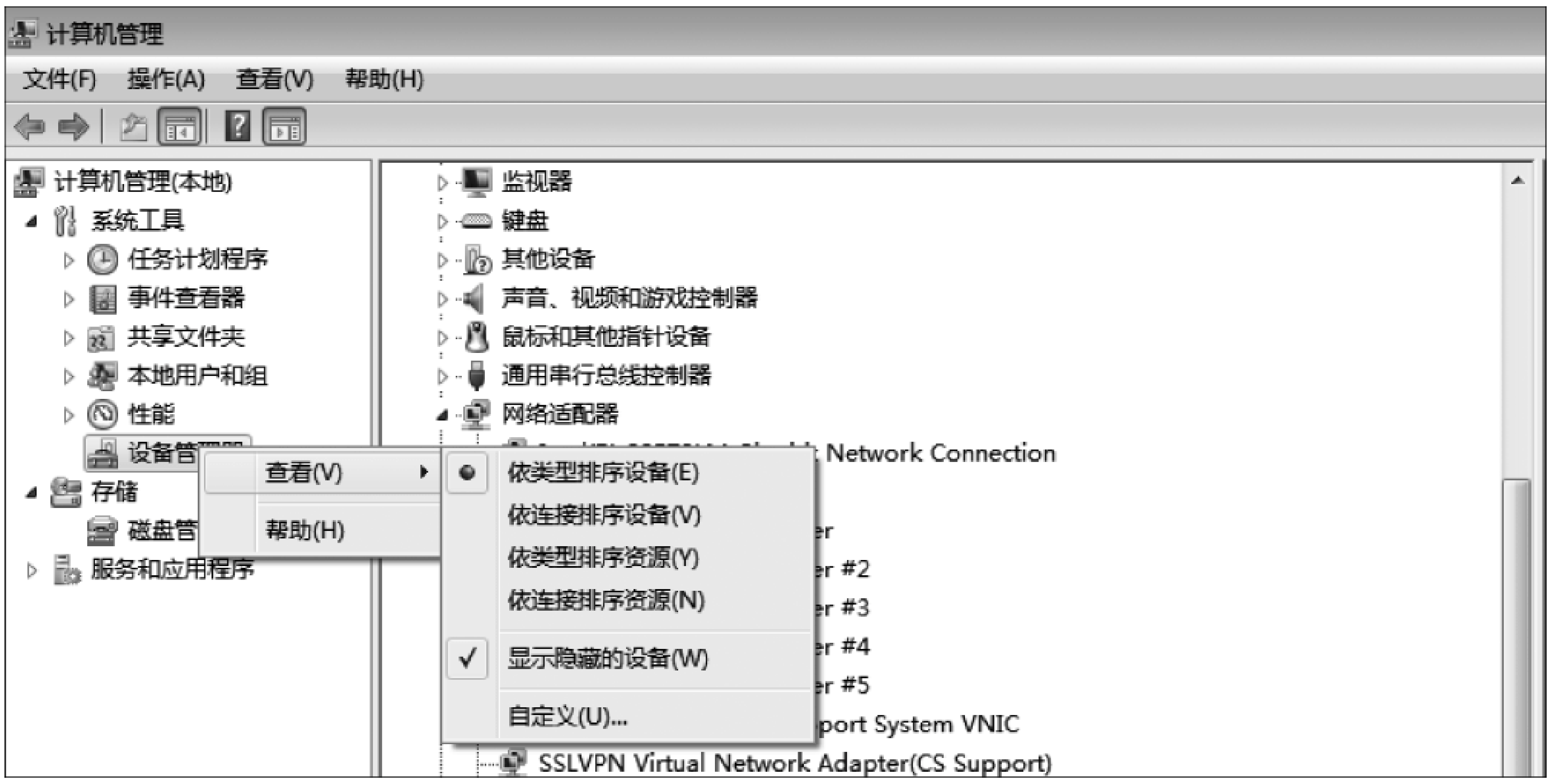


图 8-86　在系统“设备管理器”中查看网卡状态

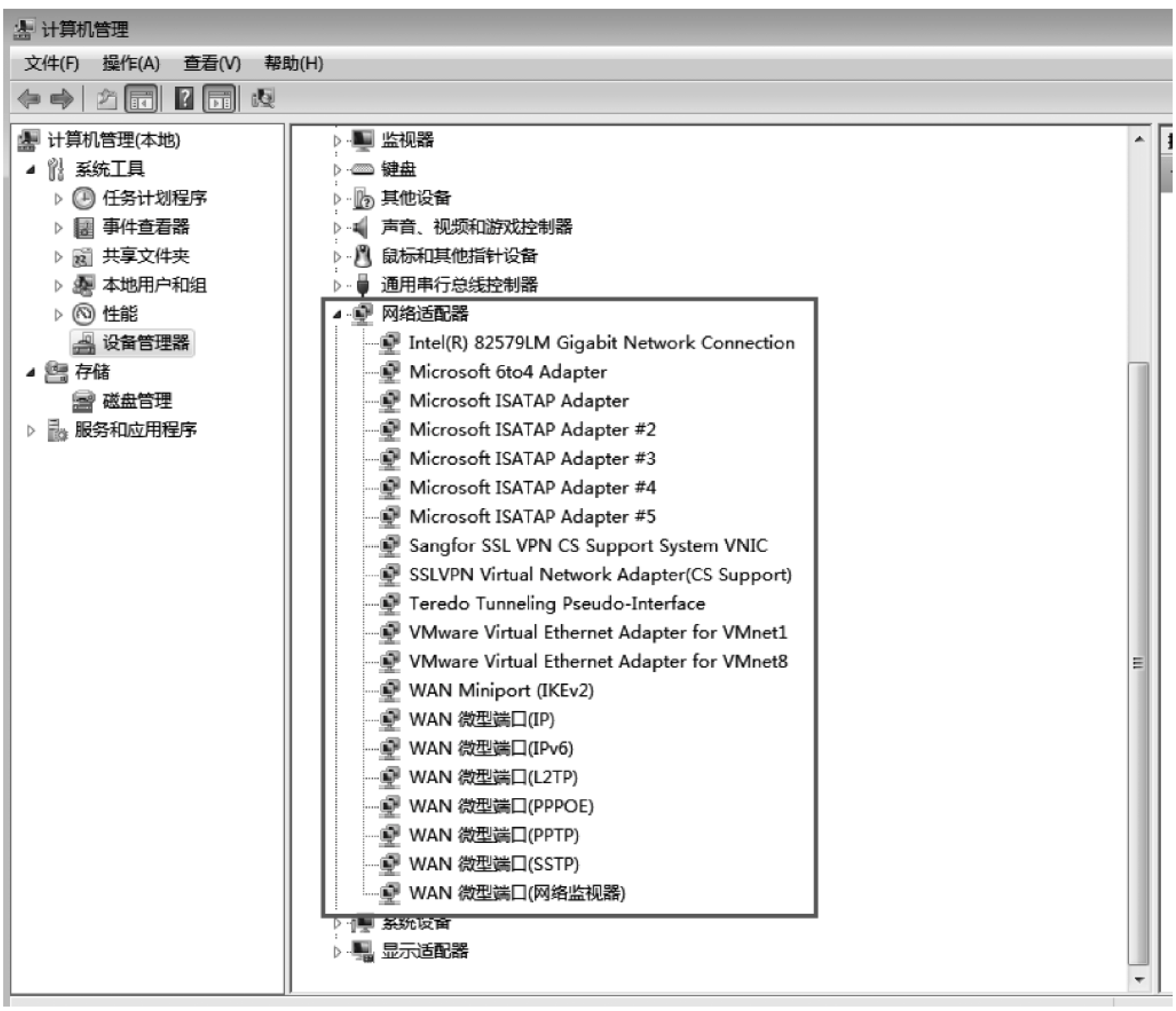


图 8-87　查看网卡状态

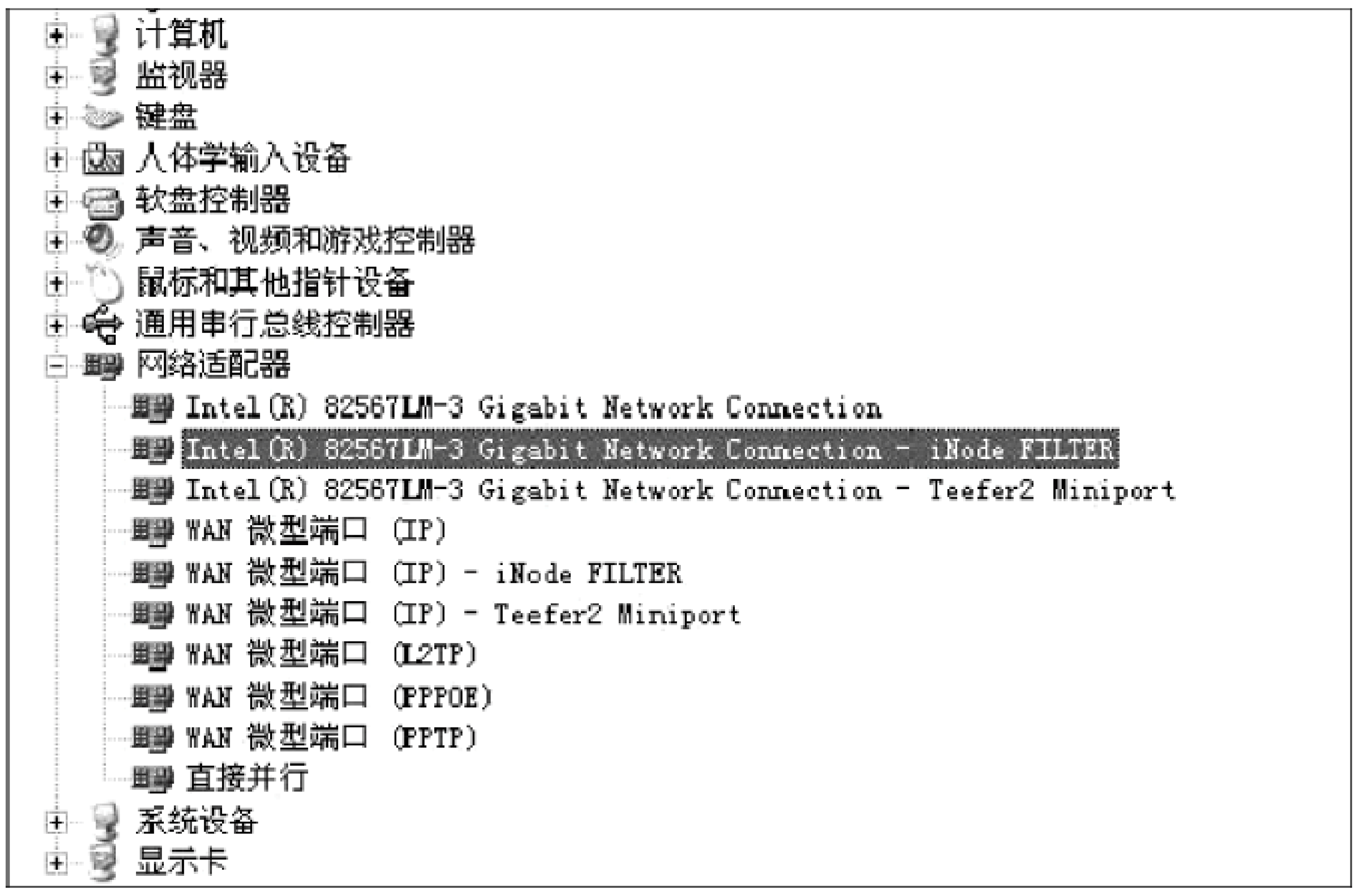


图 8-88　网卡下存在 iNode 的驱动



图 8-89　查看当前连接里的相关网络协议

说明：MD5 是一种不可逆的加密算法。首先对 iNode 安装文件进行加密取值。当传输到远端后，远端同样对 iNode 安装文件进行 MD5 加密取值。对比两个取值的结果，若一致则可判断两端的安装文件是一模一样的。MD5 检验工具下载及具体使用方法可以很容易找到相关资料，不做赘述。

(4) 终端其他软件状态检查

iNode 安装运行需要使用操作系统资源。系统资源有可能被其他软件独占甚至修改，则 iNode 无法正常调用系统资源，导致功能出现问题。

① 操作系统上的软件种类很多，建议使用排除法进行初步排查。常见有可能对 iNode 功能有影响的软件是终端防控软件、系统防火墙等。可以将这些软件禁用或关闭，观察对 iNode 功能的影响。

② 部分情况下，第三方的软件有可能对 iNode 进行破坏。即使关闭或禁用第三方软件，iNode 还是无法正常工作。这是需要卸载该软件，并且对 iNode 进行修复或者卸载重装。

说明：极端情况下，第三方软件会对 iNode 做恶意注入，导致 iNode 部分功能无法使用。可以通过进程管理工具查看，iNode 进程中调用的动态库文件中是否存在不属于操作系统和 iNode 的库文件。如图 8-90 所示为非法注入的文件。建议禁用对 iNode 进行恶意破坏的第三方软件。

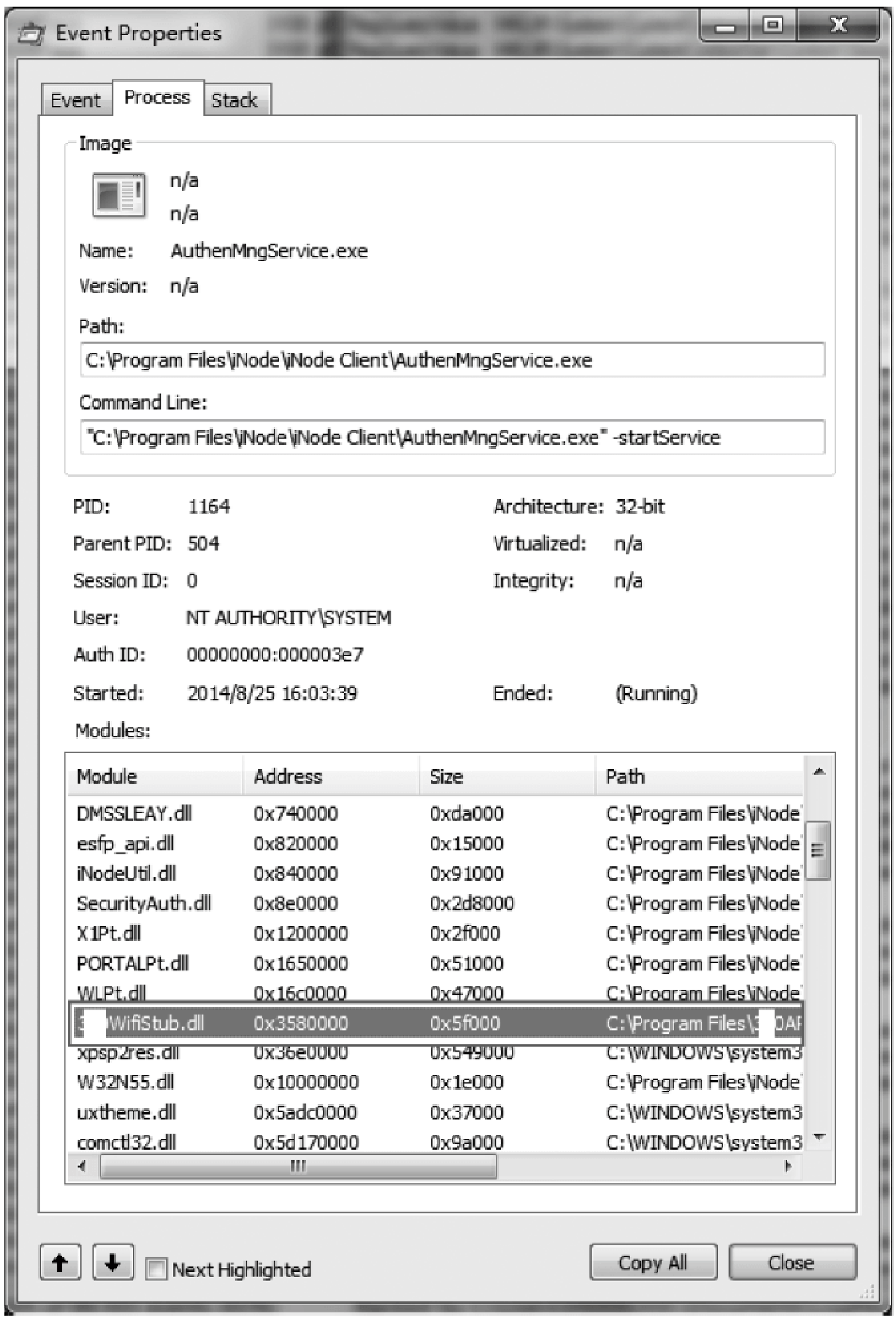


图 8-90 非法注入文件

（5）VC++ 2005 分发包检查

在 iNode 重装或升级过程中，VC++ 2005 分发包可能要进行卸载重装的操作。已安装的 VC++ 2005 分发包被未知的原因损坏的情况下，需要重新安装对其进行修复。

iNode 在重新安装或升级的过程中有可能出现如下的两个问题现象，都是 VC++ 2005 分发包损坏导致的问题，如图 8-91、图 8-92 所示。



图 8-91　VC++ 2005 分发包损坏导致问题一

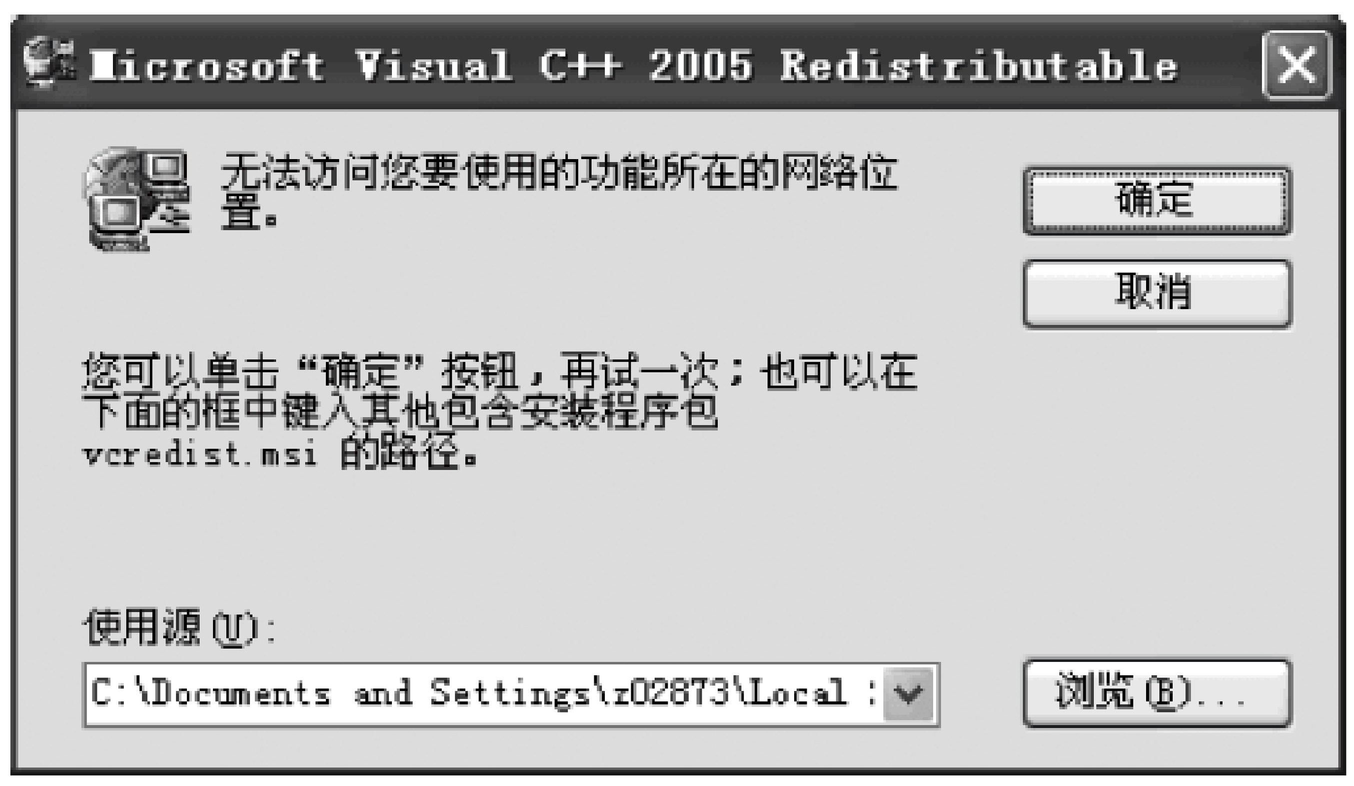


图 8-92　VC++ 2005 分发包损坏导致问题二

解决方法：在 Windows 官方网站上下载对应版本操作系统的 vcredist. msi 文件，安装修复。

说明：在公司 KMS 案例库中有处理 VC++ 2005 异常的文档案例。建议微软官网下载对应操作系统最新的 VC++ 2005 分发包文件安装修复。

（6）iNode 服务状态检查

iNode 无法启动时，若提示服务未启动或获取不到场景信息。可以检查终端上 iNode 服务的状态，如图 8-93 所示。

① 查看服务中是否有两个 iNode Service 服务，若存在则将多余的一条禁用。

② 重启 iNode Service 服务，设置该服务为自动启动。

③ 若服务无法启动，可以将 iNode 进行修复或重装。

④ 已知部分防控软件会阻止应用程序的服务启动，建议将终端安全软件禁用或关闭，或者手动将 iNode 放入安全软件的白名单中。

（7）按照具体提示寻找处理方法

安装过程或 iNode 使用中报操作系统错误，建议请咨询微软获取解决方案或检索类似问题现象进行处理。例如：下面情况的处理。

① 提示操作系统错误“Error 1935. An error occurred during the installation of assembly ... Microsoft. VC80. OpenMP，type＝"win32" ...”。请参考链接：http://www. genie9. com/

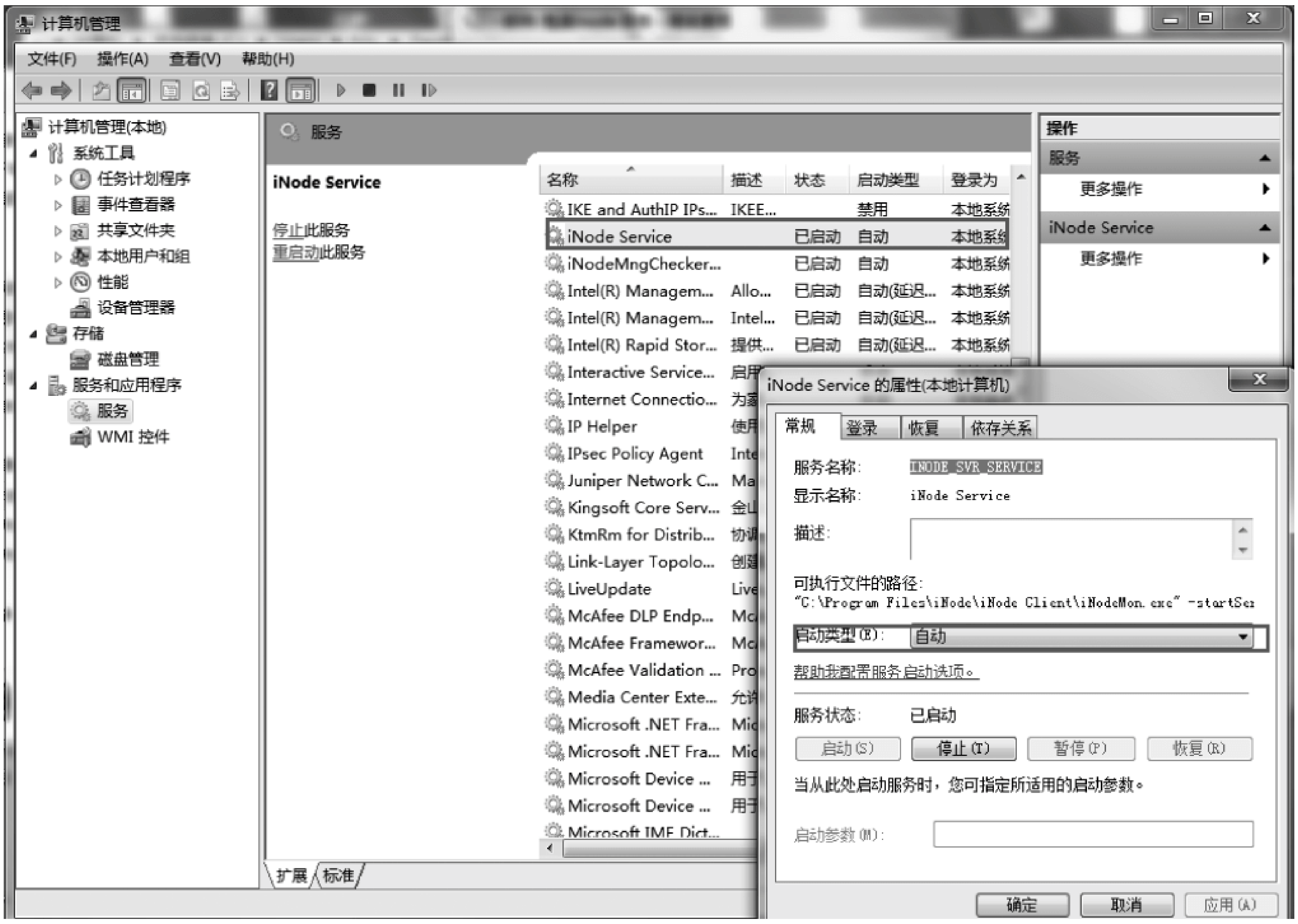


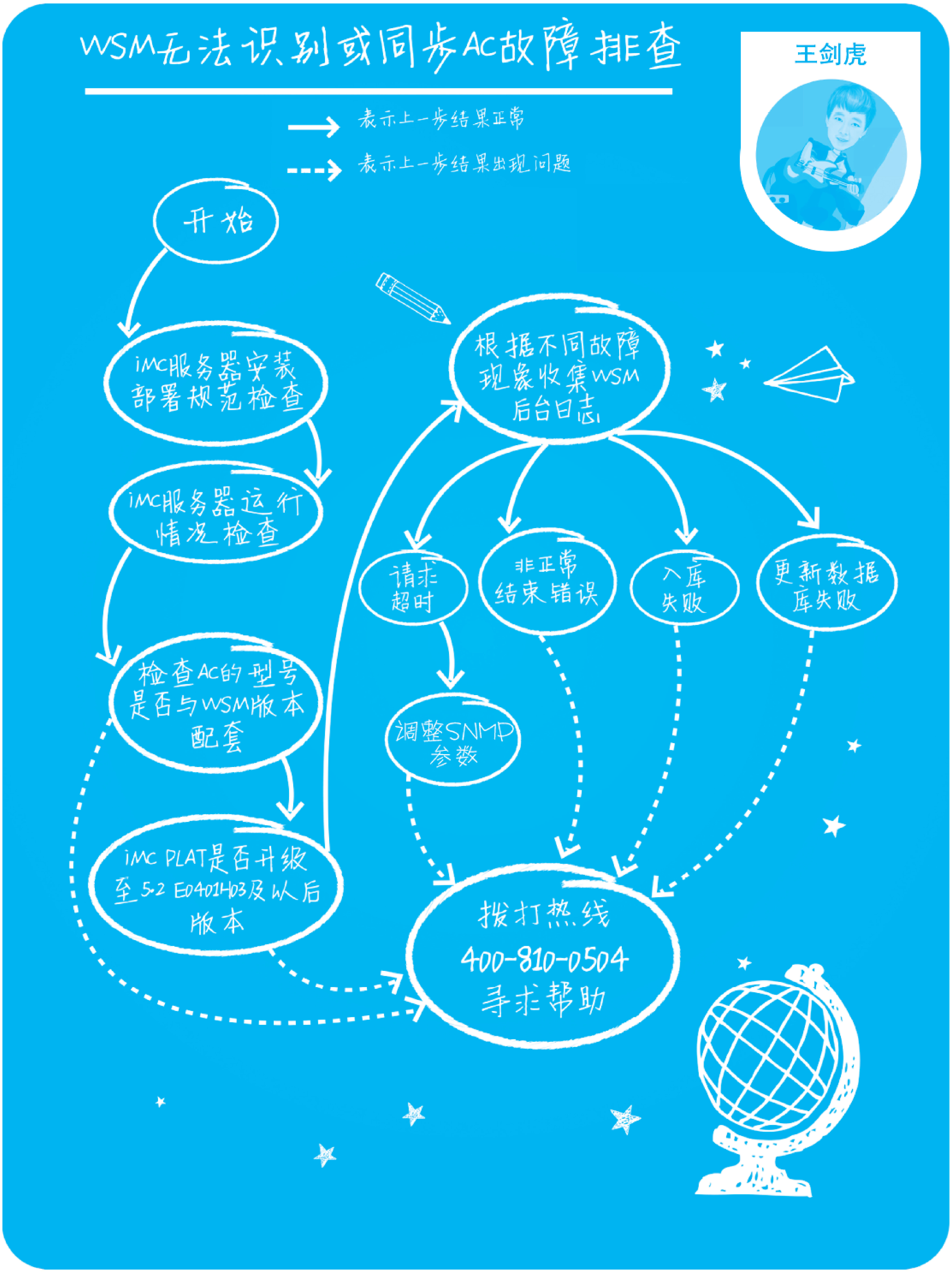
图 8-93 终端上 iNode 服务的状态

support/kb/knowledgearticle.aspx?kbid=197。

② 提示“由于应用程序配置不正确……”。请参考链接：http://jingyan.baidu.com/article/454316abb9e750f7a7c03a2a.html。

③ iNode 提示“协议初始化失败”。处理方法为：单击“开始”按钮，在开始搜索框中键入 cmd，单击“cmd.exe”按钮，单击“以管理员身份运行”按钮，然后单击“继续”按钮。在命令提示符处键入 netsh winsock reset 或 netsh winsock reset catalog，然后按 Enter 键，重启电脑。

④ iNode 提示“XML 解析器初始化失败……”。一般是由于操作系统的 XML 解析器被损坏导致的。可以管理员权限运行 CMD，在其中执行“regsvr32 /u msxml4.dll”和“regsvr32 msxml4.dll”。若还不行，则建议在微软官网上下载 msxml.msi，重装进行修复。



WSM无法识别或同步AC故障排查
王剑虎
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
检查AC的型号是否与WSM版本配套
iMC PLAT是否升级至5.2 E0401H03及以后版本
根据不同故障现象收集WSM后台日志
请求超时
非正常结束错误
入库失败
更新数据库失败
调整SNMP参数
拨打热线
400-810-0504
寻求帮助

1. 开始

WLAN(Wireless Local Area Network,无线局域网)是计算机网络与无线通信技术相结合的产物。由于 WLAN 在部署时不需要考虑复杂的布线、优化和变迁,因此 WLAN 系统便于搭建和使用,具有安装便捷、高移动性和易扩展等特点,所以其应用越来越广泛。

WSM(Wireless Service Manager)是以 iMC 平台为基础的无线服务管理系统,WSM 结合 iMC 智能管理平台,为 WLAN 管理提供了一个完善的解决方案。其中智能管理平台提供了通用的网络管理功能,WSM 则提供了无线设备相关的管理功能。

WSM 管理无线设备流程:按照常规在 iMC 平台网管中通过 SNMP 协议添加设备后,WSM 组件的资源管理中将自动出现无线设备,不需要重复添加。WSM 可以自动从平台网管中已存在的设备中发现并识别无线设备,包括 AC、FAT AP 和 FIT AP。WSM 通过设备 MIB 识别该设备是否是无线设备,具体来说要求设备支持无线网管 MIB 集。WSM 通过私有 MIB 实现对我司无线设备的网管。WSM 并不直接与 FIT AP 交互,而是通过读取无线控制器 AC 的 MIB 信息获取其下挂的 FIT AP 信息实现对 FIT AP 的管理。因此,WSM 要管理无线设备,成功添加并识别 AC 或成功同步 AC 是重要的一步。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》,检查 iMC 服务器性能是否符合配置要求。该配置是推荐的运行 iMC 最基本的部署要求,请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格,当网络中管理的 AP 数量较多,需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将 WSM 组件分布式部署在了性能良好的服务器上,重点需要检查内存占用是否过高,内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求,操作系统和数据库是否为 64 位,建议使用 64 位系统。

② 单击"开始"→"智能部署监控代理"命令,选择"部署"标签,检查"无线业务管理"功能模块是否已经部署,如图 8-94 所示。

(2) iMC 服务器运行情况检查

打开部署监控代理,查看 jserver、imcnetresdm、imcwlandm 进程是否正常启动,如图 8-95 所示。

说明:一般情况下,这些进程通过鼠标右键设置启动方式为"自动启动"。

如果无线进程 imcwlandm 启动失败,需要找到 iMC\server\conf\log\imcwlandm.log 日志,查看最后一行,一般可能有如下几种情况。

① 如果日志中出现"Initialize process enviorment failed."就是说明有其他进程占用了进程端口。检查服务器 8080、9091、161、162、61616、61626 等端口是否被 iMC 相关进程所监听,如图 8-96 所示。

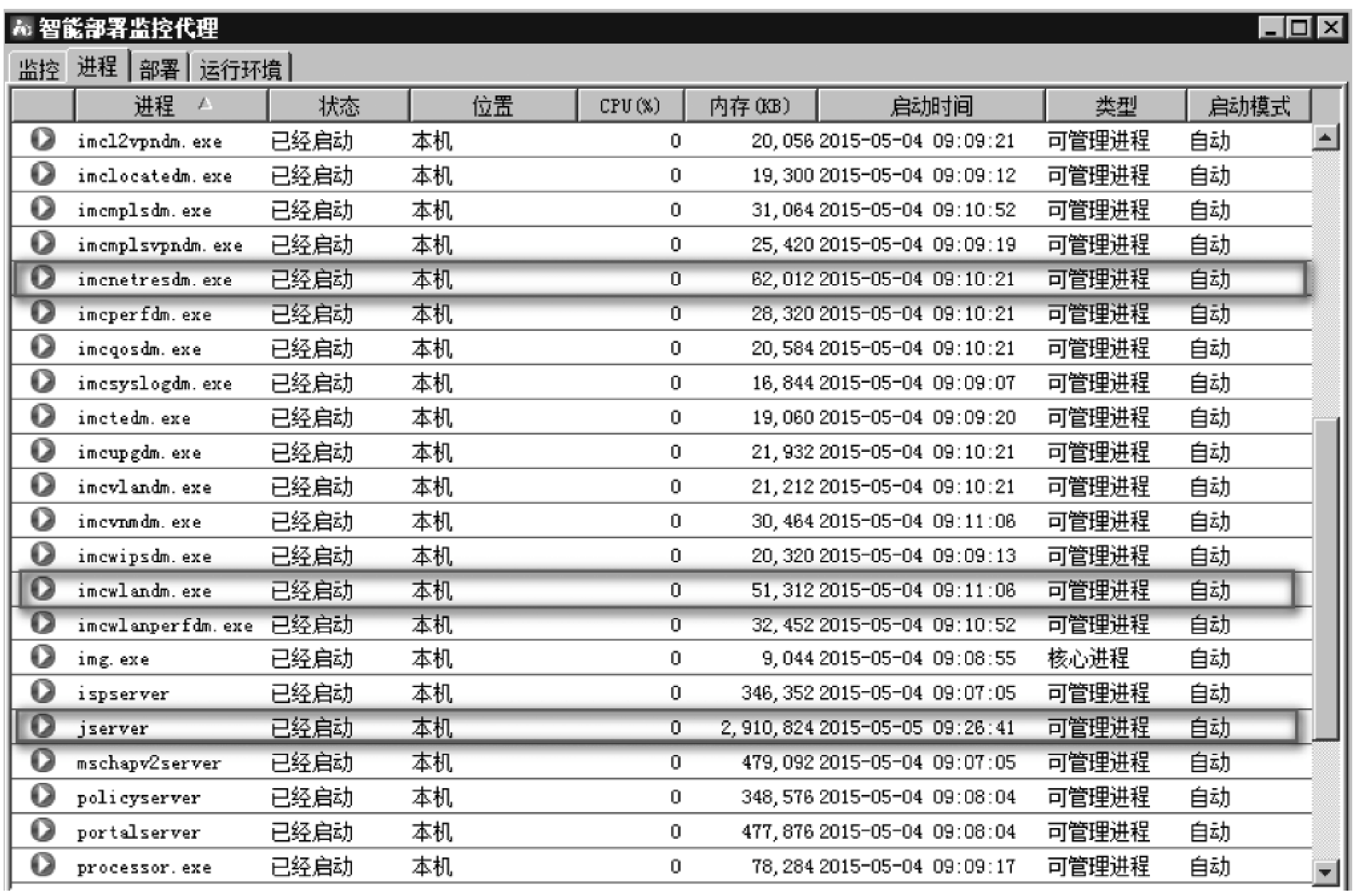

智能部署监控代理

监控 | 进程 | 部署 | 运行环境

组件名	描述	版本	状态	部署位置
智能管理平台 - 资源管理	对网络中的路由器、交换机等各类...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 告警管理	对网络进行故障监控，及时分析排...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 用户自助服务管理	对iMC的各种自助业务提供统一管理。	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 来宾接入管理	对来宾账号进行全面、智能、安全...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 智能配置中心	对网络设备进行软件升级、设备配...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 报表管理	提供各类业务报表的发布、展示和...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 网元管理	提供对数据通信设备如以太网交换...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 性能管理	对网络进行性能监控分析。	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - ACL管理	对设备进行ACL配置，实现网络数...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 网络资产管理	对网络中的设备及其配件资产进行...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 安全控制中心	监控网络中的各种事件，提供安全...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 通用搜索服务管理	对iMC的通用搜索业务提供统一管理。	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - Syslog管理	对设备Syslog进行收集、过滤、分...	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - VLAN管理	对网络中VLAN资源进行管理。	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理平台 - 虚拟资源管理	对虚拟资源进行管理。	iMC PLAT 7.1 (E0303P06)	已部署	主服务器
智能管理中心 - 无线业务管理	对iMC系统中的无线业务进行管理。	iMC WSM 7.1 (E0303P01)	已部署	主服务器
智能管理中心 - 无线入侵防御系统	用于防御未经授权的设备接入无线...	iMC WSM 7.1 (E0303P01)	已部署	主服务器
应用管理	用于监视不同种类业务的应用程序...	iMC APM 7.1 (E0301)	已部署	主服务器
分支网点管理 - 分支网点管理	对网络中的TR-069设备进行管理。	iMC BIMS 7.1 (E0301)	已部署	主服务器
分支网点管理 - 自动配置服务器	与网络中的TR-069设备进行交互，...	iMC BIMS 7.1 (E0301)	已部署	主服务器
分支网点管理 - 移动分支管理	提供对移动分支设备和业务的管理。	iMC BIMS 7.1 (E0301)	已部署	主服务器

请选择组件，按下鼠标右键激活操作菜单。

图 8-94　“无线业务管理”功能模块部署情况


智能部署监控代理

监控 | 进程 | 部署 | 运行环境

进程	状态	位置	CPU (%)	内存 (KB)	启动时间	类型	启动模式
imcl2vpndm.exe	已经启动	本机	0	20,056	2015-05-04 09:09:21	可管理进程	自动
imclocatedm.exe	已经启动	本机	0	19,300	2015-05-04 09:09:12	可管理进程	自动
imcmplsdm.exe	已经启动	本机	0	31,064	2015-05-04 09:10:52	可管理进程	自动
imcmplsvpndm.exe	已经启动	本机	0	25,420	2015-05-04 09:09:19	可管理进程	自动
imcnetresdm.exe	已经启动	本机	0	62,012	2015-05-04 09:10:21	可管理进程	自动
imcperfdm.exe	已经启动	本机	0	28,320	2015-05-04 09:10:21	可管理进程	自动
imcqosdm.exe	已经启动	本机	0	20,584	2015-05-04 09:10:21	可管理进程	自动
imcsyslogdm.exe	已经启动	本机	0	16,844	2015-05-04 09:09:07	可管理进程	自动
imctedm.exe	已经启动	本机	0	19,060	2015-05-04 09:09:20	可管理进程	自动
imcupgdm.exe	已经启动	本机	0	21,932	2015-05-04 09:10:21	可管理进程	自动
imcvlandm.exe	已经启动	本机	0	21,212	2015-05-04 09:10:21	可管理进程	自动
imcvnmdm.exe	已经启动	本机	0	30,464	2015-05-04 09:11:06	可管理进程	自动
imcwipsdm.exe	已经启动	本机	0	20,320	2015-05-04 09:09:13	可管理进程	自动
imcwlandm.exe	已经启动	本机	0	51,312	2015-05-04 09:11:06	可管理进程	自动
imcwlanperfdm.exe	已经启动	本机	0	32,452	2015-05-04 09:10:52	可管理进程	自动
img.exe	已经启动	本机	0	9,044	2015-05-04 09:08:55	核心进程	自动
ispserver	已经启动	本机	0	346,352	2015-05-04 09:07:05	可管理进程	自动
jserver	已经启动	本机	0	2,910,824	2015-05-05 09:26:41	可管理进程	自动
mschapv2server	已经启动	本机	0	479,092	2015-05-04 09:07:05	可管理进程	自动
policyserver	已经启动	本机	0	348,576	2015-05-04 09:08:04	可管理进程	自动
portalserver	已经启动	本机	0	477,876	2015-05-04 09:08:04	可管理进程	自动
processor.exe	已经启动	本机	0	78,284	2015-05-04 09:09:17	可管理进程	自动

图 8-95　查看进程是否正常启动

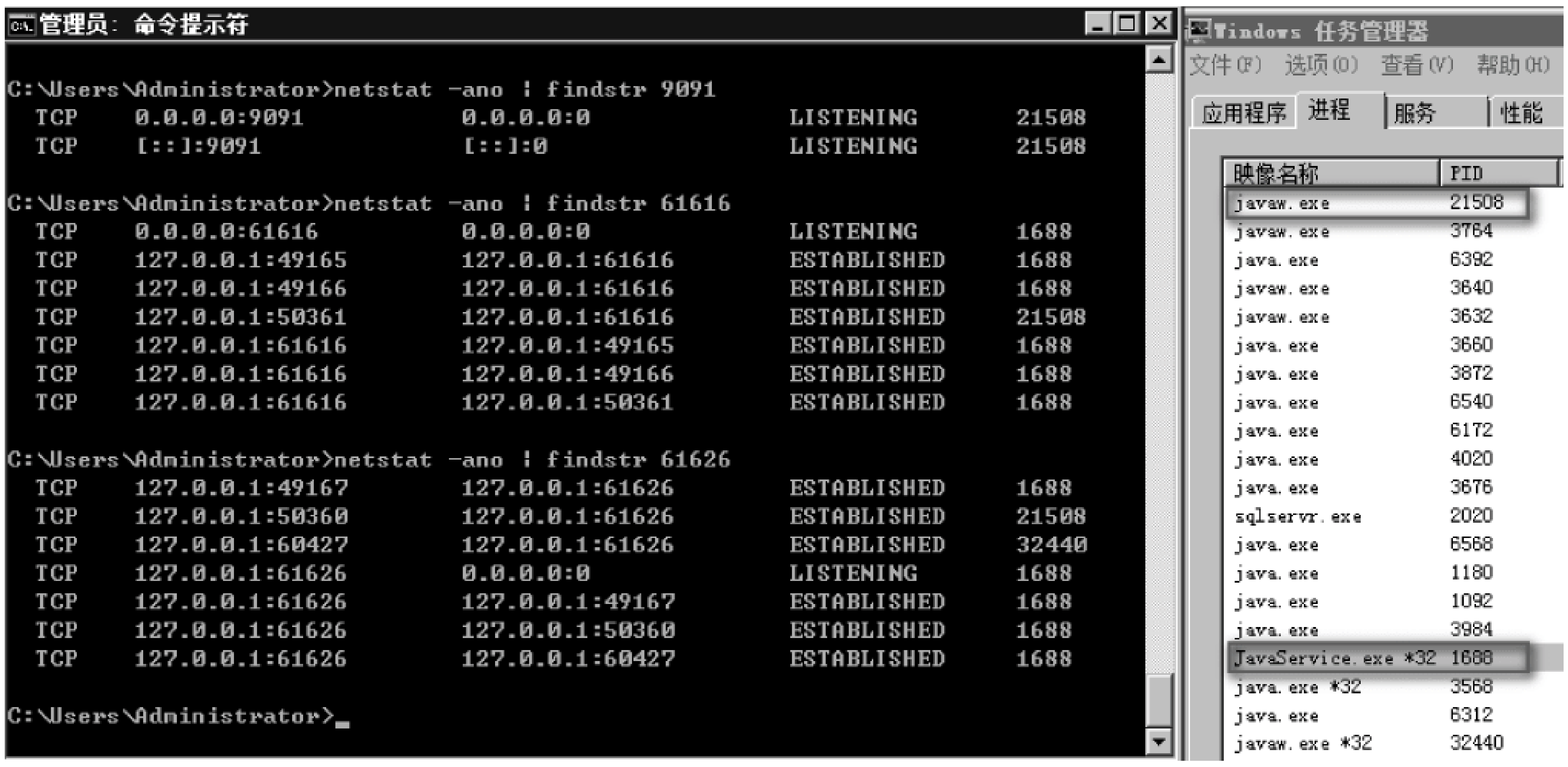


图 8-96　端口被 iMC 相关进程监听情况

说明：

(a) Windows 操作系统中，通过

netstat -aon | *findstr* ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-97 所示。

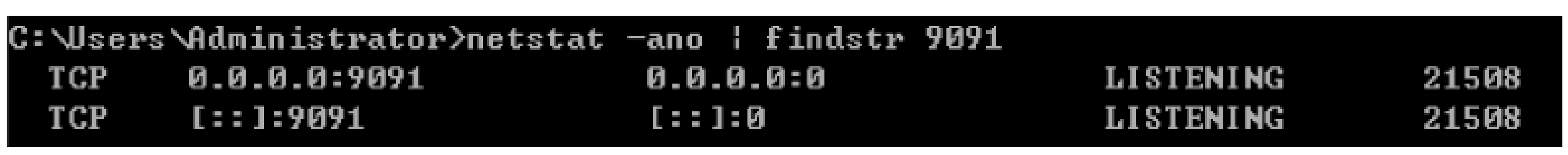


图 8-97　命令提示符回显

其中第一列 TCP 所指监听的协议，第二列 0.0.0.0:9091 所指监听的服务器的 IP 和端口号，第三列 LISTENING 代表此行信息为监听状态，最右一列 21580 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，9091 端口所对应的应为 jserver 相关的进程，61616/61626 所对应的为部署监控代理相关进程。

② 如果日志中出现 CWlanDBOper::getWlanDataDB error, db opt error!!，这个错误表示启动查表时失败，看这条语句的前三行，分析 SQL 语句是哪种错误。分析不明白的需要拨打 400 电话寻求技术支持。

③ 有一种情况只针对 Linux 的环境，如果出现 imcwlandm 进程启动失败，并且没有无线后台日志。这时候需要在 shell 中执行启动脚本，看一下具体失败原因。在 WSM 7.0 E0202P03 及之后版本，在 iMC/server/bin 文件夹下都有一个 start_wlan.sh 文件。没有的话，可以通过使用这里提供的 start_wlan.sh 文件，在当前目录中执行./start_wlan.sh 命令。

示例：使用 start_wlan.sh 脚本启动时，显示 load libfreebl3.so 错误，缺少这个文件。解决办法就是从正常的 Linux 机器中，/usr/lib/目录下拷贝 libfreebl3.so 文件到该局点 Linux 相同目录下。

(3) 检查 AC 的型号是否在 WSM 版本说明书的设备配套列表中

在添加 AC 时，首先确认在 WSM 版本说明书的设备配套列表中是否包含此 AC 型号。如果不包含，需选择合适的 WSM 版本。如果包含此型号 AC，添加后 WSM 仍无法识别，需按

照后续章节继续排查。

(4) iMC PLAT 是否升级至 5.2 E0401H03 及以后版本

iMC PLAT 5.2 E0401 版本和 WSM 配合时，对部分 AC 型号识别的不是很好，可能会出现在 iMC 中添加了 AC 但无法识别为无线设备或 WSM 无法识别的情况。这时需要将 PLAT 升级至 5.2 E0401H03 及以后版本，删除并重新添加 AC，能使 AC 得到更好的识别。如果升级后 AC 仍无法识别，需按照后续章节继续排查。

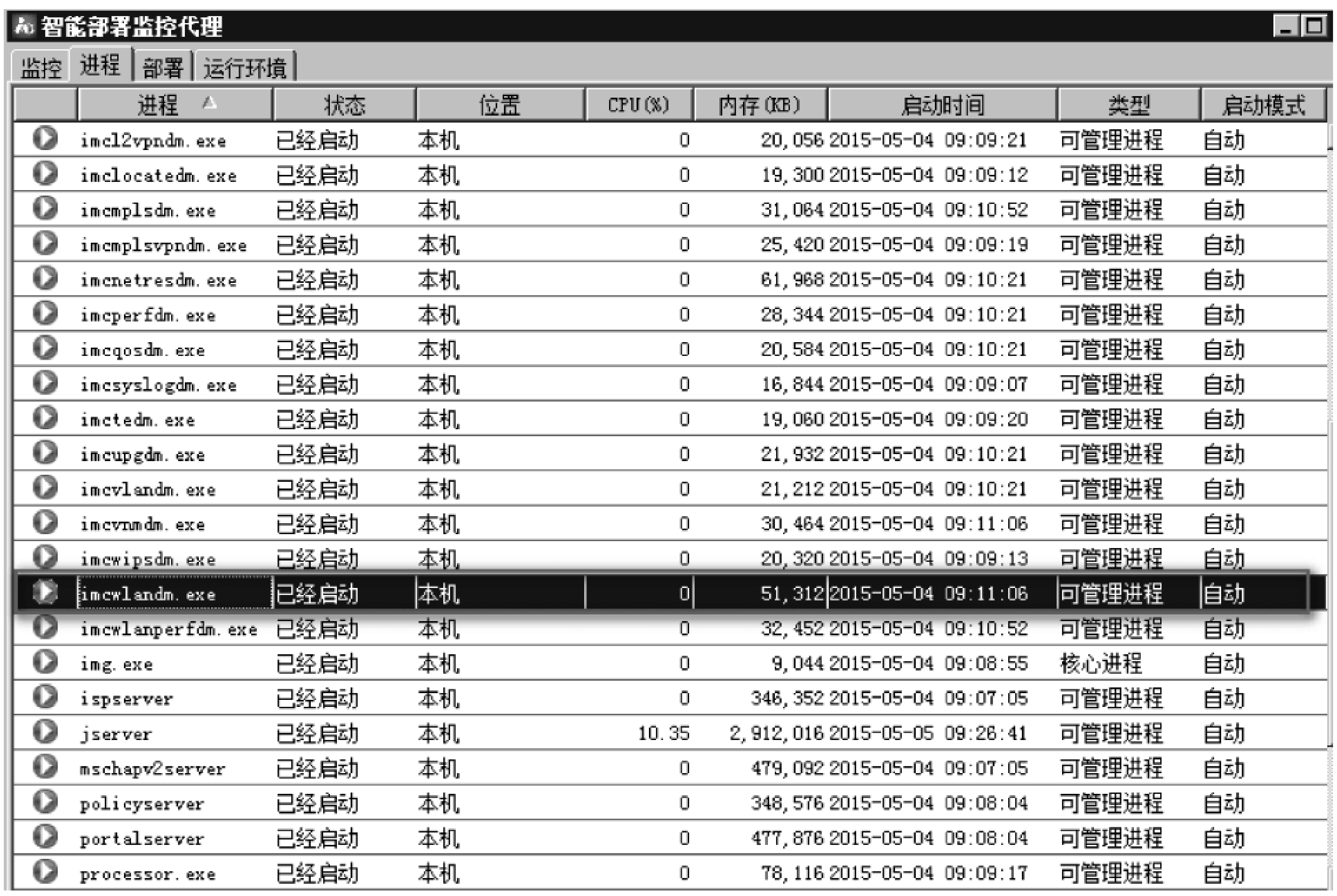
(5) 根据不同故障现象收集 WSM 后台日志

对于 WSM 无法识别/同步 AC 的故障，一般都需要分析日志来确定具体原因。一般 debug 级别日志包含的信息更多，收集方法如下。

在 C:\Program Files\iMC\server\conf 目录下打开 qvdm.conf 文件，修改其中字段。

```
#setting log level (DEBUG, INFO, WARNING, ERROR, FATAL)
    LogLevel = INFO          //该处将 INFO 修改为 DEBUG，问题解决后改回 INFO
    #setting log expire (its unit is day)
    LogExpire = 15
```

重启如图 8-98 所示进程：imcwlandm.exe。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
imcl2vpndm.exe	已经启动	本机	0	20,056	2015-05-04 09:09:21	可管理进程	自动
imclocatedm.exe	已经启动	本机	0	19,300	2015-05-04 09:09:12	可管理进程	自动
imcmplsdm.exe	已经启动	本机	0	31,064	2015-05-04 09:10:52	可管理进程	自动
imcmplsvpndm.exe	已经启动	本机	0	25,420	2015-05-04 09:09:19	可管理进程	自动
imcnetresdm.exe	已经启动	本机	0	61,968	2015-05-04 09:10:21	可管理进程	自动
imcperfdm.exe	已经启动	本机	0	28,344	2015-05-04 09:10:21	可管理进程	自动
imcqosdm.exe	已经启动	本机	0	20,584	2015-05-04 09:10:21	可管理进程	自动
imcsyslogdm.exe	已经启动	本机	0	16,844	2015-05-04 09:09:07	可管理进程	自动
imctedm.exe	已经启动	本机	0	19,060	2015-05-04 09:09:20	可管理进程	自动
imcupgdm.exe	已经启动	本机	0	21,932	2015-05-04 09:10:21	可管理进程	自动
imcvlandm.exe	已经启动	本机	0	21,212	2015-05-04 09:10:21	可管理进程	自动
imcvnmdm.exe	已经启动	本机	0	30,464	2015-05-04 09:11:06	可管理进程	自动
imcwipsdm.exe	已经启动	本机	0	20,320	2015-05-04 09:09:13	可管理进程	自动
imcwlandm.exe	已经启动	本机	0	51,312	2015-05-04 09:11:06	可管理进程	自动
imcwlanperfdm.exe	已经启动	本机	0	32,452	2015-05-04 09:10:52	可管理进程	自动
img.exe	已经启动	本机	0	9,044	2015-05-04 09:08:55	核心进程	自动
ispserver	已经启动	本机	0	346,352	2015-05-04 09:07:05	可管理进程	自动
jserver	已经启动	本机	10.35	2,912,016	2015-05-05 09:26:41	可管理进程	自动
mschapv2server	已经启动	本机	0	479,092	2015-05-04 09:07:05	可管理进程	自动
policyserver	已经启动	本机	0	348,576	2015-05-04 09:08:04	可管理进程	自动
portalserver	已经启动	本机	0	477,876	2015-05-04 09:08:04	可管理进程	自动
processor.exe	已经启动	本机	0	78,116	2015-05-04 09:09:17	可管理进程	自动

图 8-98　重启 imcwlandm.exe 进程

收集 C:\Program Files\iMC\server\conf\log\imcwlandm.yyyy-mm-dd.txt 日志。

相关操作过程的描述以及该过程的抓包。

相关问题截图。

反馈 iMC 以及 WSM 版本信息。

设备_display version 和 display cu 的配置信息。

数据库信息的收集，查看 config_db 这个数据库的 tbl_dev 表，根据 ip 可以查到 AC 的 dev_id. 这些都可以作为查找具体 AC 同步失败或失败原因的依据，如图 8-99 所示。

	dev_id	dev_type_id	dev_ip	dev_ip_mask	append_un
1	54	10354	10.153.129.64	255.0.0.0	

图 8-99 数据库

对于不同的故障现象，收集日志时的注意事项如下。

① AC 在 PLAT 中添加后，没有被平台识别为无线设备。在平台资源的设备视图下，单击同步 AC，约十分钟左右，在后台日志中搜索 pVendorDev→getWlanData error. It's not an AC device maybe. 或者 dealAddNewDev error. 当出现这些信息时才表示同步失败，可以收集日志，不然无法判断原因。

② AC 在 PLAT 中添加后，被识别为无线设备，但 WSM 中无法识别。收集日志的方式同①一样。

③ AC 在 PLAT 中添加后，被识别为无线设备，在 WSM 中可以识别，但在 WSM 中同步 AC 失败。在 WSM 的 AC 列表中，单击同步后，十分钟左右，先在后台日志中搜索 pVendorDev→getWlanData error. It's not an AC device maybe. 如果搜索不到，可以搜索 CWlanDBOper::updateWlanDataDB error，这个表示数据库更新失败。通过日志分析，一般问题出现在以上关键字的前三行内。

（6）根据日志分析故障的具体原因

根据不同的现象收集完 WSM 后台 debug 日志和抓包后，可以根据日志内容分析故障的具体原因。对于可能出现的故障日志及原因，分类如下。

① 请求超时。在日志中，如果在关键字前三行内出现“time out...”时，表示 WSM 在同步 AC 请求 get 某 mib 节点时，出现了超时。这种情况下，需要按照以下步骤排查。

（a）调整 SNMP 参数。先建议现场增加 SNMP 的超时时间，并且把 SNMP 版本调为 V1，然后尝试同步看是否能够成功。

（b）如果仍然无法同步成功，就需要拨打 400 电话寻求技术支持，由二线查看后台日志，找到出现 time out 时 WSM 在获取设备的什么内容，然后找出这些 mib 节点，在抓包中搜索这些节点，找到抓包中出现的位置，由设备侧进行定位，为何设备响应超时。示例如图 8-100 所示。

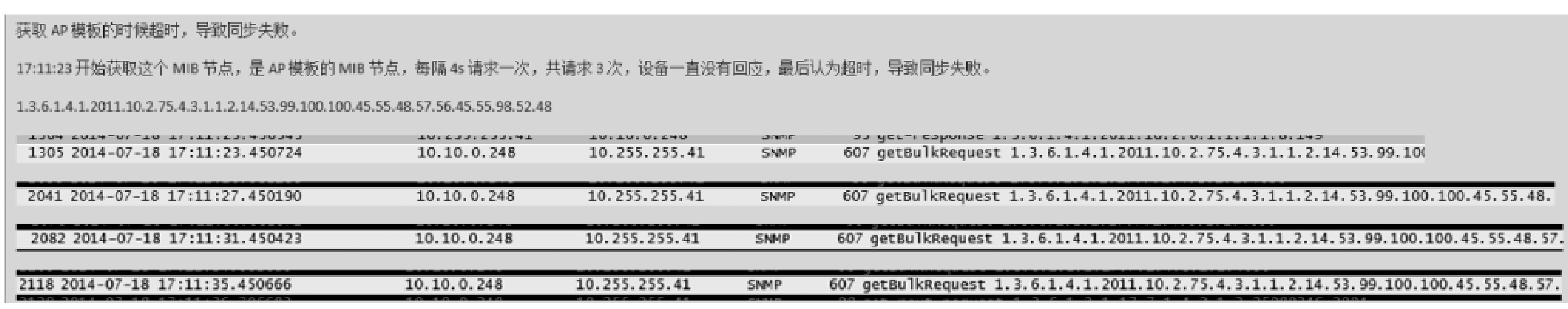
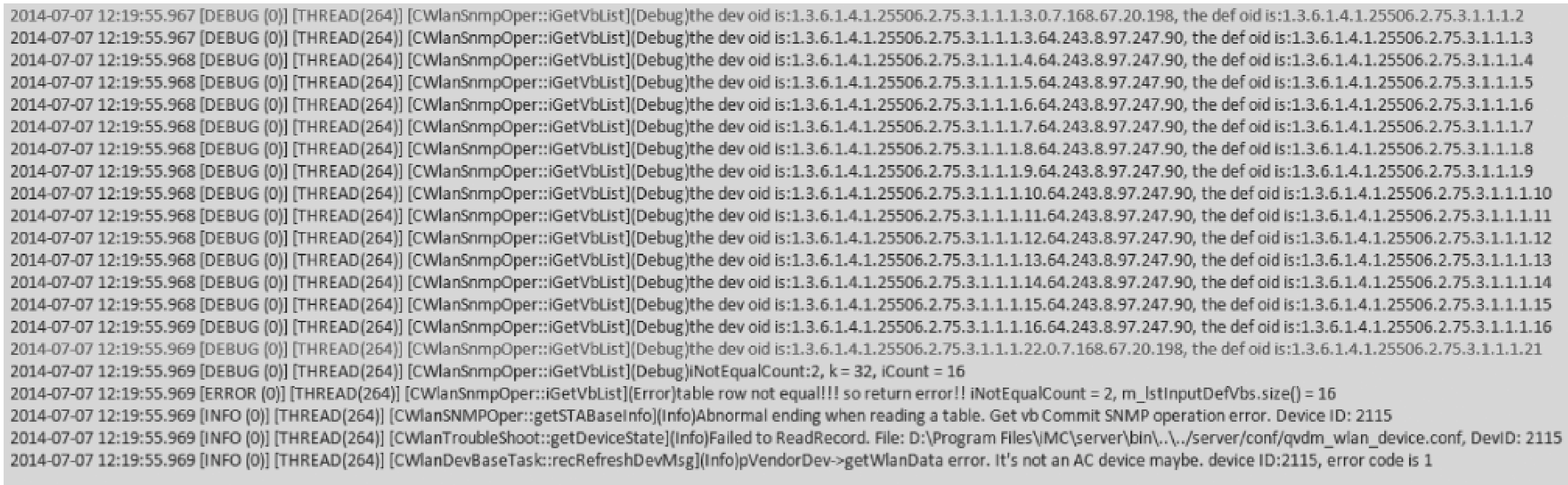


图 8-100 日志请求超时

② 非正常结束错误。当日志中出现“Abnormal ending when reading a table. Commit SNMP operation error.”时，表示此时在获取该节点时，出现了请求 OID 和设备返回 OID 不对称的现象，这种情况下需要提供 WSM 的 DEBUG 日志以及抓包，然后找到这个节点并在抓包中找到。示例如图 8-101 所示。

具体看红色文字部分，WSM 请求的 OID thedef oid is：1.3.6.1.4.1.25506.2.75.3.1.1.1.2，设备返回的 OID the dev oid is：1.3.6.1.4.1.25506.2.75.3.1.1.1.3.0.7.168.67.20.198。比较明显两个 OID 不一致，WSM 就认为同步有问题，识别 AC 失败。这种问题就属于设备问题



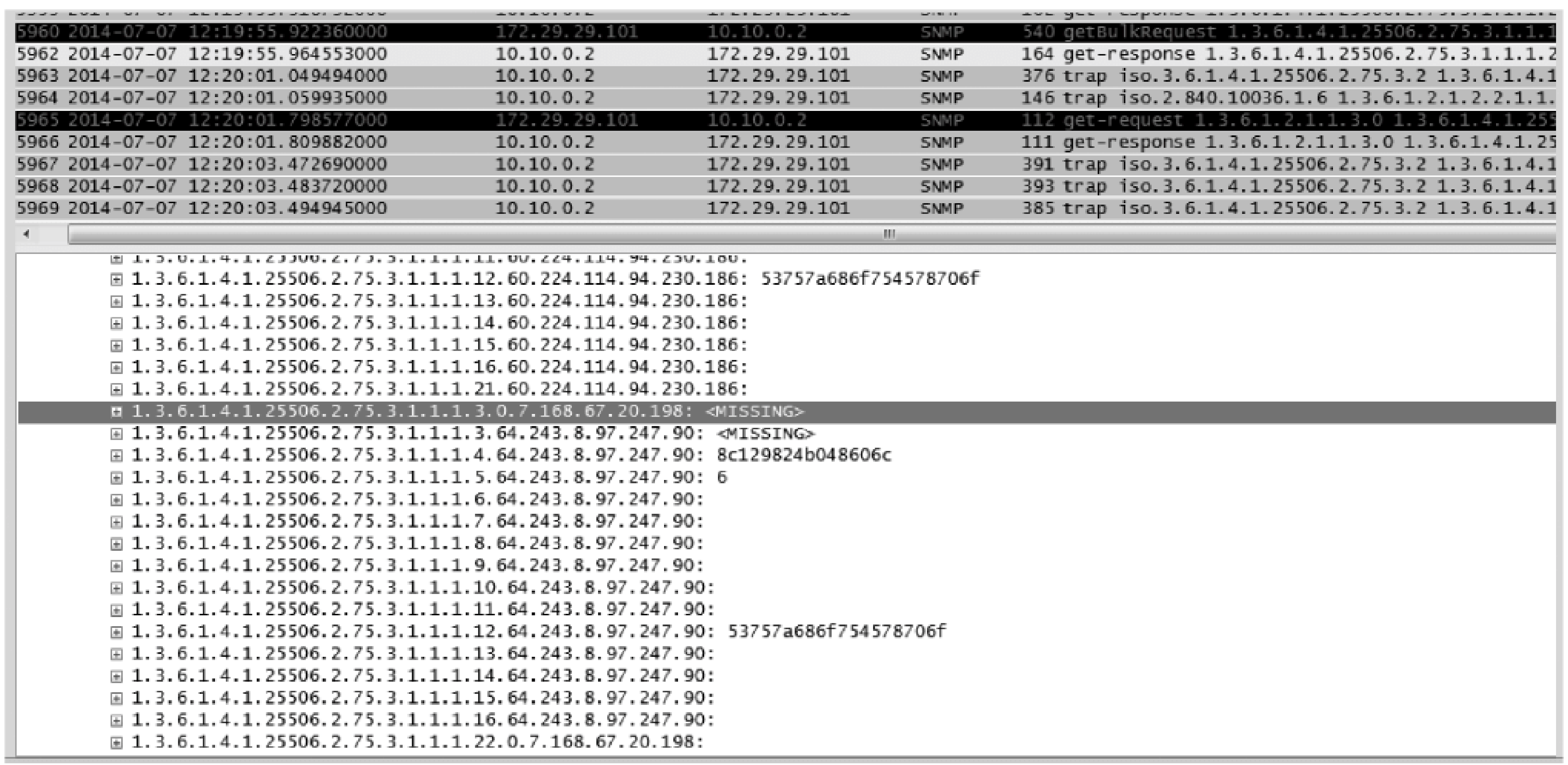


图 8-101　日志非正常结束错误

了，设备返回不正确，所以导致了 WSM 同步失败。需联系设备侧获取技术支持。

③ 入库失败。在日志中搜索 CWlanDBOper::insertWlanDataDB error，出现这种错误可以查看出错的 SQL 语句，找到具体原因。这种错误出现一种可能是升级后数据库表字段有问题，一种可能是设备返回数据有问题。示例如下。

(a) 如果 SQL 错误中出现类似这种"errorMsg: Invalid column name 'client_forward_mode.'"，这说明对应表中少了字段，可以是升级版本后数据库表字段出现了问题，需要拨打 400 电话获取进一步技术支持。

(b) 还有一种情况，可能是设备返回的数据有问题，示例如图 8-102 所示。

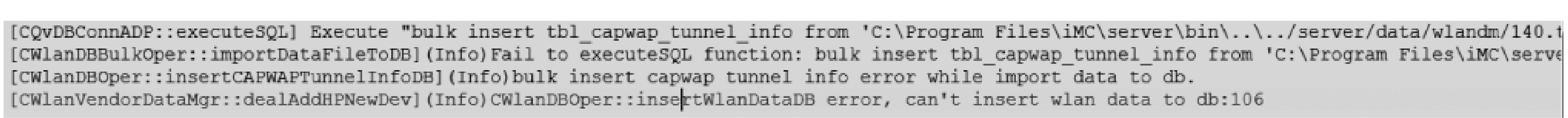


图 8-102　设备返回数据有问题

第一句如下。

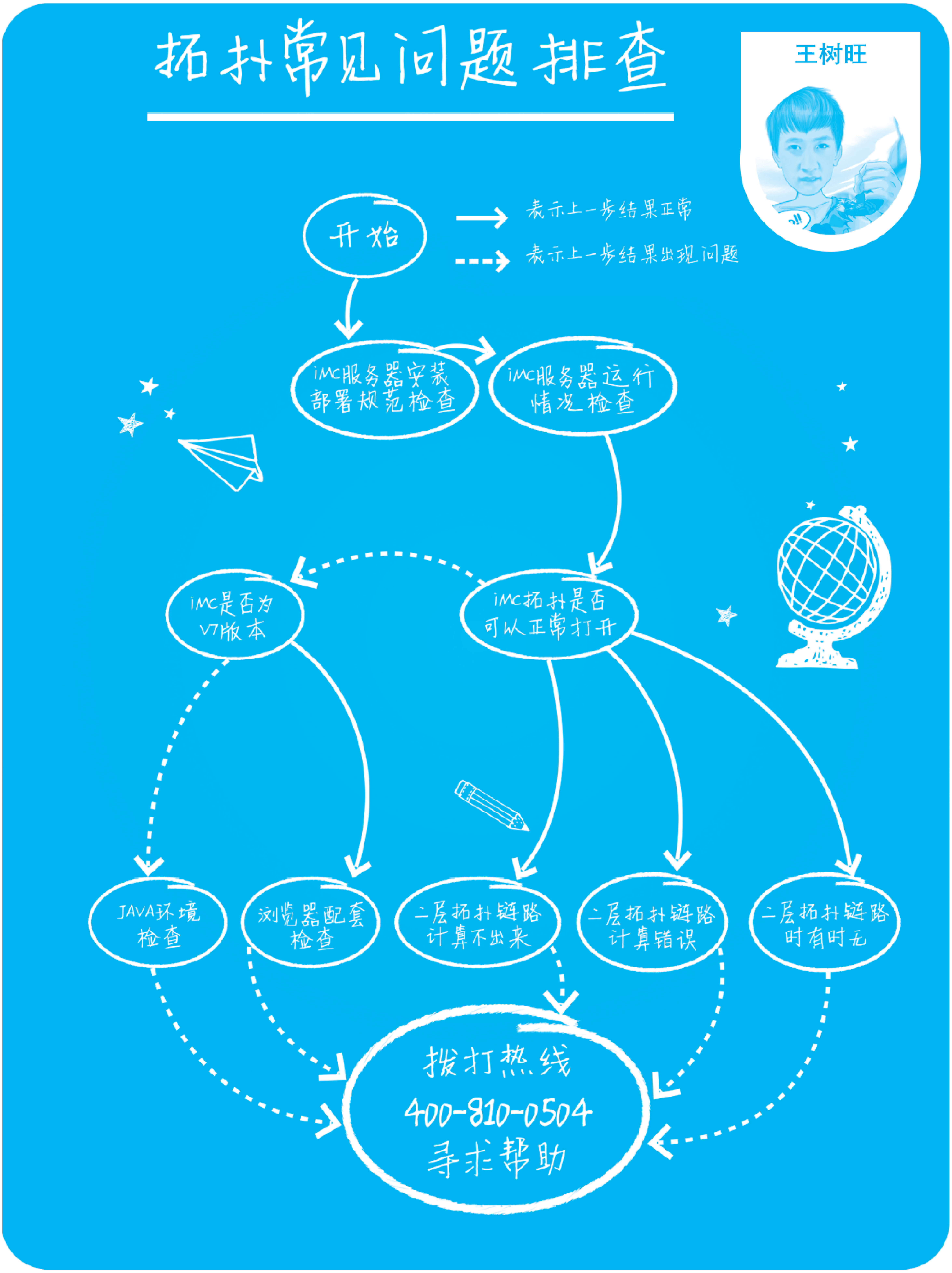
```
[CQvDBConnADP::executeSQL] Execute "bulk insert tbl_capwap_tunnel_info from 'C:\Program Files\iMC\server\bin\..\../server/data/wlandm/140.txt' with (FIELDTERMINATOR = ',|', ROWTERMINATOR = '\n')" failed, errorMsg: Violation of PRIMARY KEY constraint 'PK__tbl_capw__C003D25002C769E9'. Cannot insert duplicate key in object 'imc_wsm.tbl_capwap_tunnel_info'. The duplicate key value is (00:00:00:00:00:00, 106).
```

通过第一句 SQL 错误，可以看出来是在向数据库表 tbl_capwap_tunnel_info 中插入数据时，出现了主键冲突，具体为什么会主键冲突，就需要分析这个 140.txt 文件了。所以需要收集这个文件，然后通过 400 电话联系二线获取进一步的技术支持。

举例中的 140.txt 文件如下，可以看出前面的字段有问题，全是 00：00：00：00：00：00，需要通过日志甚至代码来确认，是获取哪个字段得到的，然后查看设备返回的信息是否就是这样，如果是的话就是设备侧有问题。需联系设备侧继续定位。

```
00:00:00:00:00:00,|68,|0,|75474,|0,|75474
00:00:00:00:00:00,|68,|0,|75465,|0,|75465
00:00:00:00:00:00,|68,|0,|75472,|0,|75472
00:00:00:00:00:00,|68,|0,|75465,|0,|75465
00:00:00:00:00:00,|68,|0,|75470,|0,|75470
00:00:00:00:00:00,|68,|0,|75465,|0,|75465
```

④ 更新数据库失败。如果设备已经加入了 WSM 管理，但是在 WSM 中同步 AC 失败，并且搜索到 CWlanDBOper::updateWlanDataDB error。这说明 WSM 在同步 AC 时，很有可能是设备上返回的数据出现问题，导致入库失败。这与上述第③点入库失败问题类似，根据找到出错的 SQL 分析是哪种错误。必要时需通过 400 电话联系产品线二线获取技术支持。


拓扑常见问题排查
王树旺
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC拓扑是否可以正常打开
iMC是否为V7版本
JAVA环境检查
浏览器配套检查
二层拓扑链路计算不出来
二层拓扑链路计算错误
二层拓扑链路时有时无
拨打热线
400-810-0504
寻求帮助

1. 开始

随着网络设备越来越多，组网越来越复杂，当网络出现故障时，网络管理员根据网络结构迅速定位网络问题的难度越来越高。因此对一个网络管理员而言，完全掌握一个网络结构对于后续的维护工作是非常重要的。iMC 二层拓扑能够准确计算设备间的连接关系，并以全网拓扑的方式进行展示，方便网络管理员查看。

在 iMC 平台中，基础链路包括两类：IP 拓扑链路和二层拓扑链路。IP 拓扑链路主要是利用路由器或三层交换机的路由接口地址计算出来的链路，如果两个路由接口子网地址和掩码都相同，则这两个路由接口都会创建一条链路连接到它们的公共子网上。如果公共子网的掩码长度为 30 位，则两个路由接口之间将会形成一条直连链路(PPP)。IP 拓扑链路体现的是路由器或三层交换机在 IP 层的子网划分和连接关系，是一种逻辑链路。二层拓扑链路是利用设备间的邻居协议或 MAC 地址学习关系计算出来的链路。邻居协议包括 LLDP、NDP、CDP、STP，这些协议都会记录对端设备信息，iMC 基于这些对端设备信息直接计算出二层拓扑链路。对于 MAC 地址学习关系计算方式，iMC 从设备中采集 BRIDGE-MIB 和 Q-BRIDGE-MIB 数据，并计算设备间 MAC 地址学习记录的交集关系，如果交换机能够彼此学习到对方，且交集为空，则认为两台交换机之间存在链路。和 IP 拓扑链路不同，二层拓扑链路体现的是设备间的物理连接关系。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

(2) iMC 服务器运行情况检查

要想正常 iMC 拓扑功能需要保证 iMC 进程运行正常。

单击“开始”→“智能部署监控代理”命令，选择“进程”标签，查看进程 jserver 和 imcl2topodm 是否正常启动，具体如图 8-103 所示。

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(3) iMC 拓扑是否可以正常打开

iMC 拓扑是通过客户端浏览器访问打开的，常见问题包括浏览器无法打开 iMC 拓扑。如果无法打开拓扑，请按照下面的(4)、(5)、(6)条排查；如果可以访问链路识别有问题，请按照(7)、(8)、(9)条排查。

(4) iMC 是否为 V7 版本

iMC V7.0 版本开始，增加 HTML 5 拓扑功能，有原来的 Java 拓扑逐步向 HTML 5 拓扑变更；所有如果现场使用的是 V7.0 版本之前的 iMC，现场需要按照第(5)条检查 Java 环境；如果是 7.0 及以后版本请使用 HTML 5 拓扑，也就是资源下的网络拓扑功能打开拓扑，现场需要按照第(6)条排查。

(5) Java 环境检查

在使用 Java 拓扑的情况下，打开 iMC 拓扑时需要检查你客户端的 Java 版本是否满足

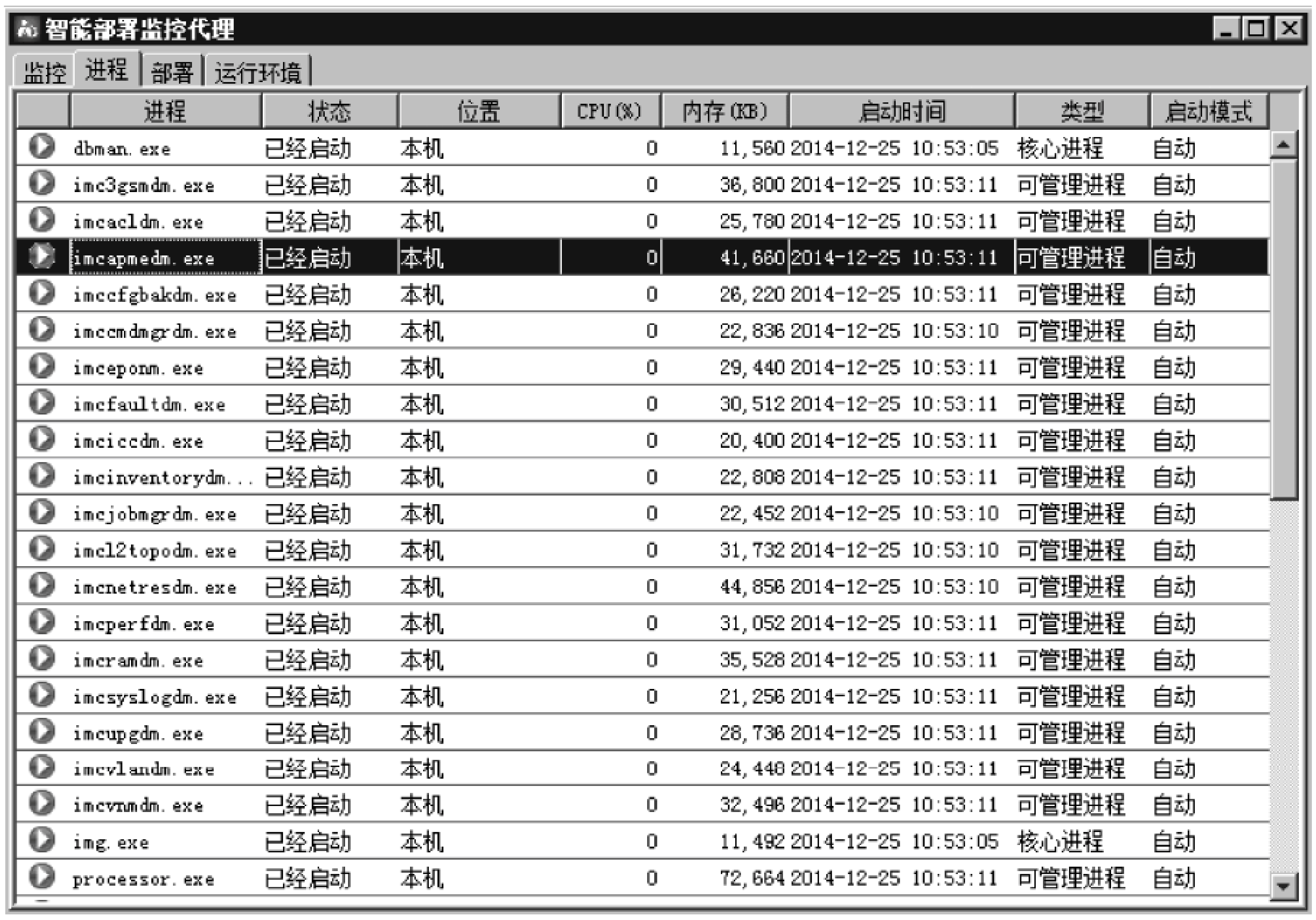


图 8-103 “进程”标签

iMC的要求,这个在打开拓扑时有体现。

另外,在安装了Java环境的客户端无法打开Java拓扑时,请检查你的Java安全级别和在例外站点中增加拓扑的URL,方法如下。

① 打开客户端的控制面板,双机Java图标,如图8-104所示。



图 8-104 客户端的控制面板

② 在 Java 控制面板中将安全级别调整到底或高。并在例外站点中增加拓扑的 URL 单击“应用”按钮，然后重启浏览器继续访问 iMC 拓扑，如图 8-105 所示。

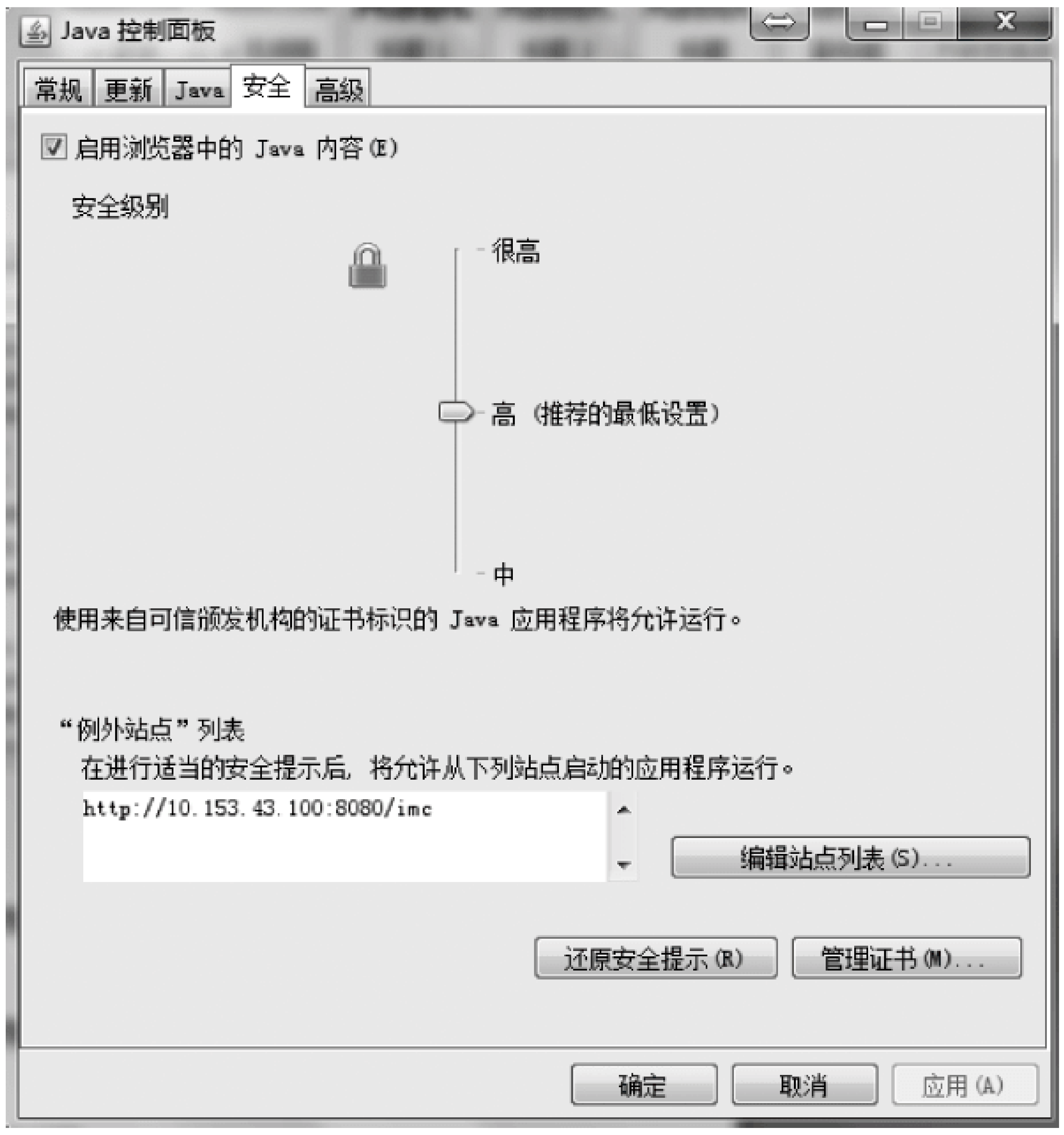


图 8-105　Java 控制面板

(6) 浏览器配套检查

在使用 HTML 5 拓扑的情况下，需要注意我们 iMC 登录界面提示，使用满足要求的浏览器版本，建议使用 Chrome35 及以上版本的浏览器。

(7) 二层拓扑链路时有时无

① 错误现象。现场经常遇到拓扑上的两台设备间的链路初始计算是正确的，但过了一段时间后，链路消失或变成虚线。再过段时间，链路可能又能正确计算。

② 问题定位。这种二层拓扑链路有时能计算出来，有时又计算不出来的现象称之为链路老化(Aged)。原因是这条链路的计算方式为 MAC 地址学习，而 MAC 地址学习信息是周期老化的，在 MAC 地址老化(Aged)的情况下，链路计算不出来；在 MAC 地址未老化的情况下，链路可以正确计算。

③ 解决办法。为了解决设备 MAC 地址学习信息老化的问题，iMC 会周期发送伪造 ping 报文、iMC 还支持 DISMAN-PING。不过，DISMAN-PING 是比较新的标准，很多老设备不支持。开启的位置在 iMC 的 Web 界面中的系统参数中，默认开启。针对不支持的设备或不能开启该功能的客户，建议在设备上启用 LLDP 协议。

(8) 二层拓扑链路计算不出来

① 错误现象。两台设备之间从组网上看有一条链路，但 iMC 没有计算出来。以设备 10.153.89.194 和 10.153.89.200 为例，10.153.89.194 和 10.153.89.200 之间从组网来看有一条链路，但 iMC 显示两台设备之间没有链路。

② 问题定位。出现本问题的原因很多，需要通过二层拓扑内存数据文件进行定位。

按照本章节“附录一”提供的方法获取二层拓扑链路内存数据，并提取和 10.153.89.194、

10.153.89.200 相关的内存信息。

在文本文件 10.153.89.200.txt 中查找 10.153.89.194 的 MAC 地址 00:e0:fc:1d:82:5e、0xe0fc1d825e，发现 10.153.89.200 的邻居信息和 MAC 地址学习信息中都没有 10.153.89.194 的 MAC 地址，因此这两台设备之间的链路不可能从 10.153.89.200 发起计算。在 10.153.89.194.txt 中查找 10.153.89.200 的 MAC 地址 00:e0:fc:3d:b9:7d、0xe0fc3db97d，发现 10.153.89.194 具有相关的学习信息。

```
MacAddress learn Info:
                …
                IfIndex: 8
                IfDesc: Ethernet0/8
                0xe0fc3db97d
                0xe0fc3db97d
```

由于 10.153.89.200 没有学习到 10.153.89.194，不满足按照 MAC 地址学习计算方式的相互学习条件，因此不能计算出这两台设备之间的链路。

尽管 10.153.89.200 和 10.153.89.194 直连，但 10.153.89.200 学习不到 10.153.89.194 的 MAC 地址，基本可以肯定的是 10.153.89.200 学习的 MAC 地址信息已经被老化了。

③ 解决方法。参见第 7 节的解决方案。

(9) 二层拓扑链路计算错误

① 错误现象。两台设备之间本来没有任何链路，但 iMC 却计算出一条链路。以设备 10.153.89.98 和 10.153.89.116 为例，10.153.89.98 和 10.153.89.116 之间从组网来看并没有链路，但 iMC 却计算出两者之间有一条链路。

② 问题定位。该问题出现的原因很多，必须通过二层拓扑内存数据文件进行定位。

按照本节“附录一”提供的方法获取二层拓扑链路内存数据，并提取和 10.153.89.98、10.153.89.116 相关的内存信息。

在文本文件 10.153.89.98.txt 和 10.153.89.116.txt 中，确实记录了这样一条链路，当然，这两个文件中记录的是同一条链路，因为 LinkID 相同。

```
------------------------10.153.89.98.txt------------------------
DevID: 12
SymbolID: 1017
IP: 10.153.89.98
…
Macs:
0xe0fc003100
…
MacAddress learn Info:
…
IfIndex: 4227858
IfDesc: Ethernet1/0/30
0xfe2498048
0xfe2498048
…
LinkInfo:
…
LinkID: 149 LinkLeftSymbolID: 1017 LinkRightSymbolID 1010 LinkLeftIfDesc: Ethernet1/0/30
LinkRightIfDesc: Ethernet4/8 LinkType: 0 LinkCaclType: 3
```

说明：LinkID 149 的右符号 ID 为 1010，就是 10.153.89.116 的 SymbolID。

```
------------------------10.153.89.116.txt------------------------
DevID: 7
SymbolID: 1010
IP: 10.153.89.116
…
Macs:
0xfe2008048, 0xfe21da613, 0xfe21da614, 0xfe2498048
…
MacAddress learn Info:
IfIndex: 10
IfDesc: Ethernet4/8
0x111101, 0xfe1111111, 0xfe2000009, 0xe0fc001001, 0xe0fc003100, 0xe0fc020003, 0xe0fc067a80,
0xe0fc075880, 0xe0fc107fde, 0xe0fc107fe1, 0xe0fc211314, 0xe0fc30c8be, 0xe0fc4450f8, 0xe0fc5131cf,
0xe0fc52f006, 0x123456789012
0x111101, 0xfe1111111, 0xfe2000009, 0xe0fc001001, 0xe0fc003100, 0xe0fc020003, 0xe0fc067a80,
0xe0fc075880, 0xe0fc107fde, 0xe0fc107fe1, 0xe0fc211314, 0xe0fc30c8be, 0xe0fc4450f8, 0xe0fc5131cf,
0xe0fc52f006, 0x123456789012
…
LinkInfo:
LinkID: 149 LinkLeftSymbolID: 1017 LinkRightSymbolID 1010 LinkLeftIfDesc: Ethernet1/0/30
LinkRightIfDesc: Ethernet4/8 LinkType: 0 LinkCaclType: 3
```

说明：LinkID 149 的左符号 ID 为 1017，就是 10.153.89.98 的 SymbolID。

由于这条链路是通过 MAC 地址学习信息计算出来的(LinkCaclType：3)，按照 MAC 地址学习计算方式进行计算，设备 10.153.89.98 通过接口 Ethernet1/0/30 学习到设备 10.153.89.116 的 MAC 地址 0xfe2498048；10.153.89.116 通过接口 Ethernet4/8 学习到设备 10.153.89.98 的 MAC 地址 0xe0fc003100；10.153.89.98 接口 Ethernet1/0/30 学习到的所有 MAC 地址和 10.153.89.116 接口 Ethernet4/8 学习到的所有 MAC 地址交集为空。由于按照 MAC 地址学习计算方式的 3 个条件都已经满足，因此 iMC 二层拓扑链路计算本身没有问题。

③ 解决办法。需要确认 10.153.89.98 和 10.153.89.116 中间是哪一台设备，为什么它们没有学习到中间那台设备的 MAC 地址。经过查看网络确认，在 10.153.89.98 和 10.153.89.116 中间的那一台设备是 10.153.89.101，10.153.89.101 未加入到 iMC 中。由于设备 10.153.89.101 没有启动任何邻居协议，不会主动和其他设备通信，导致 10.153.89.98 和 10.153.89.116 的学习信息中没有 10.153.89.101 的 MAC 地址。把设备 10.153.89.101 加入 iMC 后，手工同步 10.153.89.98、10.153.89.101、10.153.89.116，问题得到解决。

(10) 附录一

在某些情况下，客户可能不愿意提供数据库，如果 iMC 是 R2602P01 及以后的版本(R2602 及以前的版本二层拓扑链路不支持内存导出)，此时可以获取 iMC 二层拓扑链路的内存数据。

获取 iMC 二层拓扑链路的内存数据过程如下。

① 在 CMD 模式下进入 iMC 安装目录。

② 设置 IMCROOT 环境变量。

③ 进入调试命令所在目录\iMC\server\bin，并执行 imfcmd 3 16 -f12topo.txt，如图 8-106 所示。

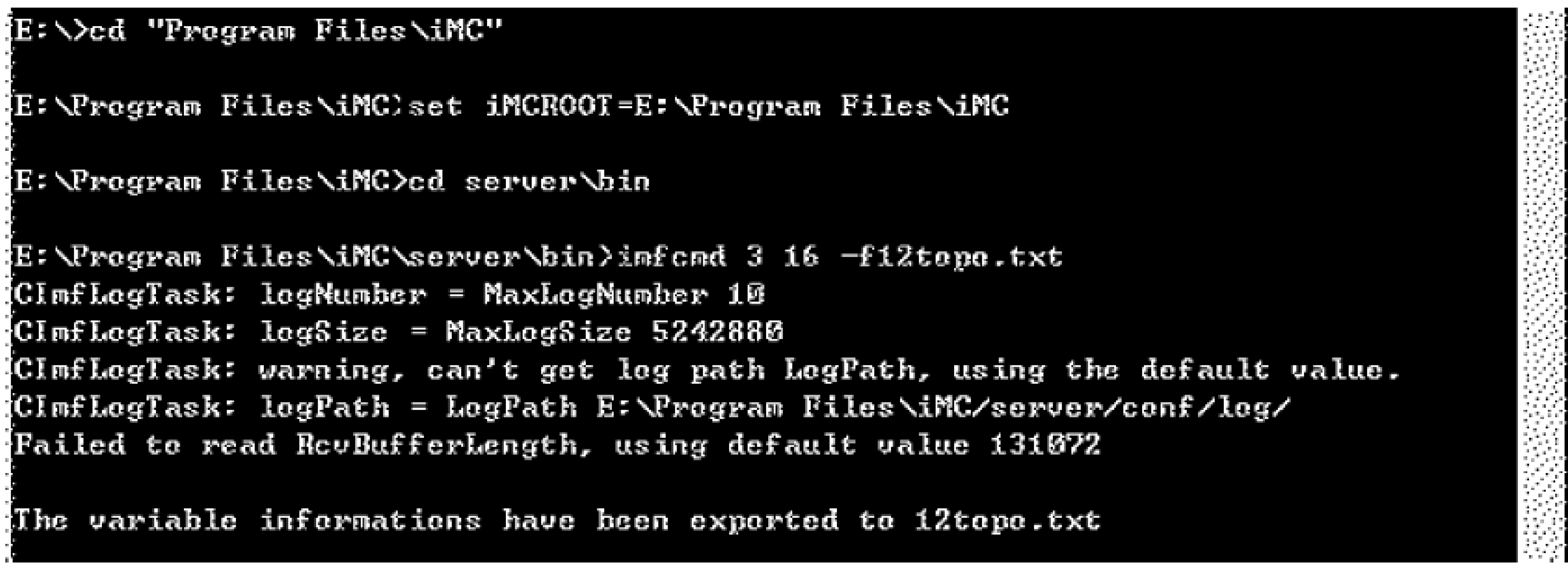
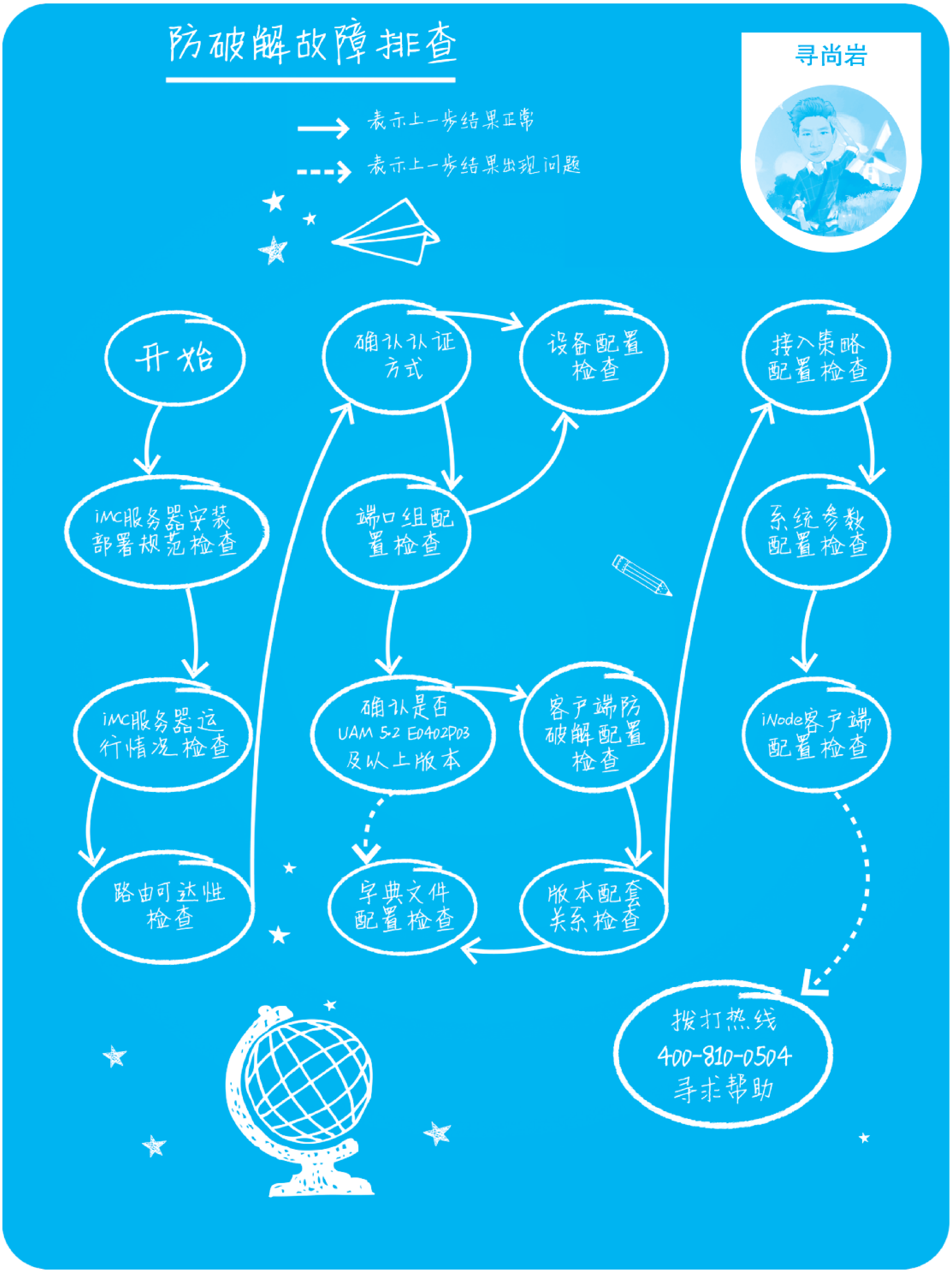


图 8-106　进入调试命令

命令执行结束以后，将在\server\bin 目录下产生一个 12topo.txt 文件，该文件包含所有当前的二层拓扑链路内存信息。


防破解故障排查
寻尚岩
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
路由可达性检查
确认认证方式
设备配置检查
端口组配置检查
确认是否UAM 5.2 E0402P03及以上版本
客户端防破解配置检查
字典文件配置检查
版本配套关系检查
接入策略配置检查
系统参数配置检查
iNode客户端配置检查
拨打热线 400-810-0504 寻求帮助

1. 开始

对于计费局点，往往有用户使用非法客户端认证上线，然后使用代理软件共享上网，H3C iNode 防破解功能可以防止使用仿冒的认证客户端认证上网，避免了代理上网行为；对于有安全检查的局点，使用仿冒客户端可以逃过安全检查，启用防破解功能后同样可以避免这种现象。iNode 防破解问题有启用防破解后用户不能上线及用户上线后防破解功能不生效两种，对于防破解问题定位故障的思路及顺序是：UAM 侧服务器软硬件状态及路由可达性检查、确认认证方式、防破解参数配置检查和 iNode 配置检查。

本文举例组网如图 8-107。

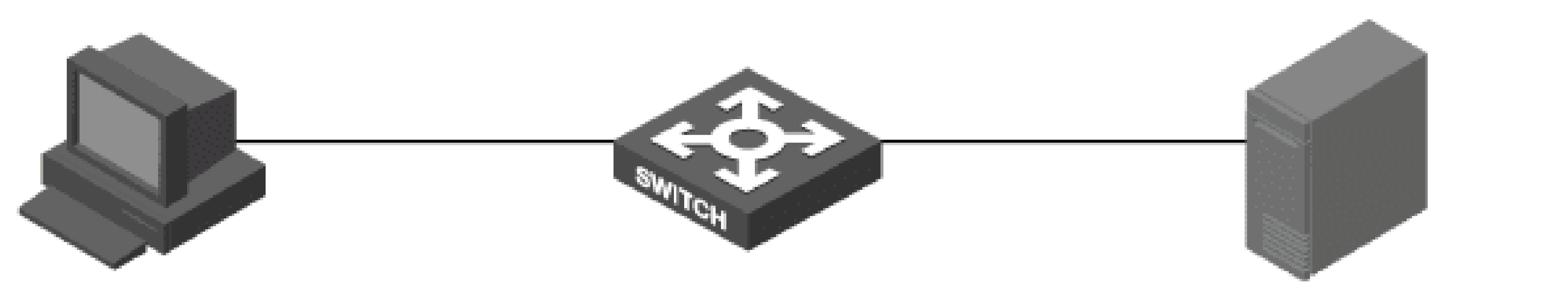


图 8-107　组网举例

IP 规划如下。

认证终端 PC：172.16.16.2/24，网关 172.16.16.1。

认证设备：VLAN 16：172.16.16.1/24，VLAN 100：172.16.100.1/24。

iMC 服务器：172.16.100.61/24，网关 172.16.100.1。

2. 流程图相关操作说明

（1）iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题时首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、同时在线人数多，则需要根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”“策略服务器”“策略代理服务器”和“智能策略代理”组件状态应为“已部署”，如图 8-108 所示。

（2）iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程，各进程是否正常为“已经启动”。

① 在部署监控代理中，查看 uam.exe、ispserver、policyserver 进程是否正常启动；如果是 Portal 认证方式还需要确认 portalserver 进程正常启动，如图 8-109 所示。

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。



图 8-108 查看部署页面

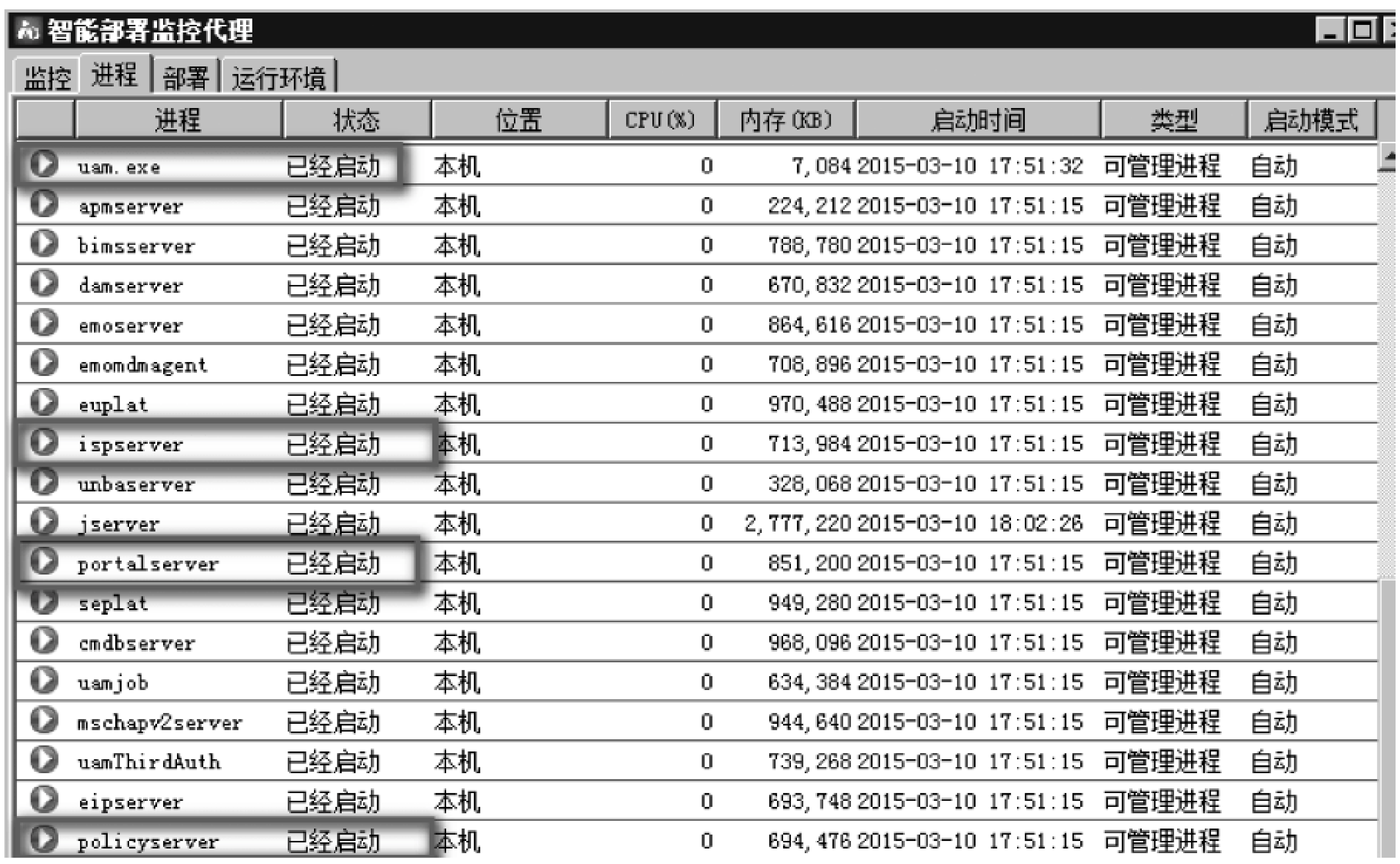


图 8-109 查看各进程是否正常启动

(b) Portalserver 提供 Portal 认证功能。

(c) Policyserver 主要用来提供客户端类功能。

(d) Uam 进程提供用户认证功能。

(e) Ispserver 统一代理与 iNode 客户端的通信。

② 检查 iMC 服务器 1812、1813、9019、50100 和 50200 UDP 端口是否被上述相关进程监听，如图 8-110 所示。

说明：

(a) Windows 操作系统中，通过

netstat -aon | findstr :端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

(b) 1812、1813 所对应的进程 PID 应为 uam 相关的进程。



图 8-110　各端口被进程监听情况

(c) 1812、1813 对应的 IP 应为 UAM 服务器实际 IP 地址。

(d) 9019 端口所对应进程 PID 为 Policyserver 相关进程，所对应的 IP 地址应为 0.0.0.0。

(e) 50100、50200 端口所对应进程 PID 为 Portal 相关进程，所对应的 IP 地址应为 0.0.0.0。

(f) Linux 系统命令

Netstat -apn | grep：端口号。

③ 检查“iMC 智能监控代理”→“运行环境”选项卡，数据库连接状态是否正常，如图 8-111 所示。

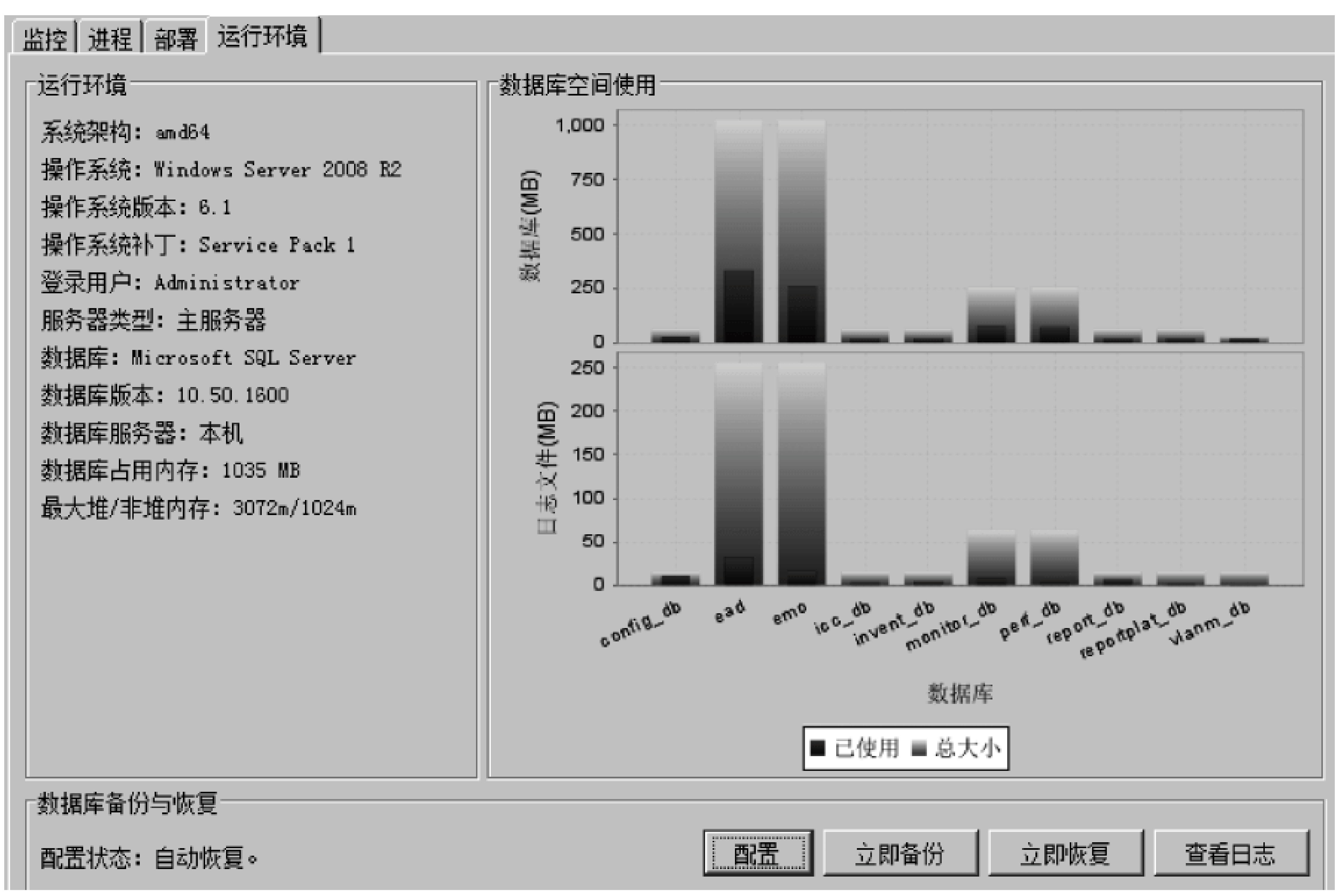


图 8-111　数据库连接状态

（3）路由可达性检查

单击“用户”→“用户接入管理”→“接入设备管理”命令，需添加接入设备发给 iMC 服务器 Radius 协议报文的端口 IP，iMC 默认会同该 IP 进行 Radius 协议报文交互，需保证 iMC 可以 ping 通该 IP，本例中接入设备 IP 应为 172.16.100.1。

对于 Portal 认证场景，需要保证认证前后认证客户端和 Portal 服务器路由可达，保证 Portal nas-ip 和 Portal 服务器路由可达，Portal nas-ip 默认为用户网关 172.16.16.1。

说明：

① 接入设备会有多个 IP 地址，如果要更改接入设备 IP，需在 radius scheme 视图下配置如下命令，iMC 侧需同步修改如下。

[sw-radius-h3c] nas-ip 172.16.2.1，并在 iMC 上更改为 172.16.2.1。

② Portal 认证方式更改 portal nas-ip 后需在 interface-vlan 视图下配置命令，iMC 侧需同步修改如下。

[5400eac -Vlan-interface6]portal nas-ip 192.168.6.1。

（4）确认认证方式

iNode 防破解功能需要与 802.1x 或 Portal 认证结合，不同的认证方式防破解配置项不同；如果是 802.1x 认证，请参考本文排查步骤（5）；如果是 Portal 认证方式，请参考本文排查步骤（6）。

（5）设备配置检查

本文对认证相关的基本配置不做赘述，只是针对防破解功能所需特殊配置进行检查。对于 802.1x 认证，要求认证方案必须为扩展模式，且设备端口下必须配置 dot1x 握手安全，相关命令如下。

```
[BAS-radius-h3c]display this
 radius scheme h3c
 server-type extended-------配置为扩展模式
 primary authentication 172.16.100.61
 primary accounting 172.16.100.61
 key authentication 123
 key accounting cipher 123
 nas-ip 172.16.100.1
 [BAS-Ethernet1/0/1]dot1x handshake secure—启用握手安全
```

说明：

① 防破解功能要求必须配置扩展模式。

② 接入设备配置的 key 值需与 iMC 侧接入设备配置的 key 值保持一致。

③ Portal 认证方式下同样需要认证方案为扩展模式。

（6）端口组配置检查

Portal 认证时如果要启用防破解功能，需要在端口组开启“客户端防破解”功能，如图 8-112 所示。

（7）确认是否 UAM 5.2 E0402P03 及以上版本

不同版本的 UAM 需要配套不同版本的 iNode 客户端，否则防破解功能不生效。需要在 iMC 配置管理台“关于”里面查看 UAM 的版本，当 UAM 版本高于等于 5.2 E0402P03 时参考



图 8-112　开启客户端防破解功能

本文排查步骤(8),低于该版本时参考排查步骤(9)。

(8) 客户端防破解配置检查

5.2 E0402P03 及以上 UAM 版本需要单击“用户”→“接入策略管理”→“业务参数配置”→“系统配置”→“客户端防破解配置”命令后的页面中配置 iNode 管理中心 IP 地址,且状态为“已生效”,如图 8-113 所示。



图 8-113　配置 iNode 管理中心 IP 地址

说明:

① UAM 5.2 E0402P03 及以上版本防破解功能配套的 iNode 最低版本为 iNode 5.2 E0406。

② 配置的管理中心 IP 地址的服务器必须安装 iNode 管理中心,且版本必须和 iNode 版本保持一致,最低为 iNode 5.2 E0406。

③ 管理中心 IP 地址状态必须为“已生效”;正常情况单击左上“生效”按钮后,UAM 会将此 iNode 管理中心的特征值写入数据库,确认其他配置无误后如果防破解功能还不生效,可以多次单击“生效”按钮再次测试。

④ 现网中如果存在不同版本的 iNode 客户端,可以在此页面配置多个 iNode 管理中心 IP 且版本与 iNode 保持配套即可。

(9) 字典文件配置检查

UAM 版本低于 5.2 E0402P03 且 iNode 版本低于 5.2 E0406 时需要在 iMC 配置管理台

“业务”→“用户接入管理”→“业务参数配置”→“客户端防破解”页面配置防破解字典文件，字典文件存放在 iNode 管理中心安装路径“Program Files\iNode\iNode Manager\dictionary\＊”处，名称为 yyyymmdd-001.hz、yyyymmdd -002.hz 和 yyyymmdd -003.hz，分别对应 Windows、Linux 和 Mac OS 三种操作系统，当网络中存在多个 iNode 版本时，可以导入多个不同版本的 iNode 字典文件以使所有合法客户端都可以正常上线。

(10) 版本配套关系检查

防破解功能要求的配套版本如下。

UAM 5.2 E0402P03 以下版本必须配套 iNode 5.2 E0406 以下版本；UAM 5.2 E0402P03 及以上版本配套 iNode 5.2 E0406 及以上版本；如果配套关系不满足，防破解功能不生效。

(11) 接入策略配置检查

防破解功能需要在单击“用户”→“接入策略管理”→“业务参数配置”→“系统配置”→“系统参数配置”命令后的页面中选择“仅限 iNode 客户端”单选框，如图 8-114 所示。



图 8-114　接入策略配置检查

说明：

① 客户端最低版本限定了网络中可以使用的最低 iNode 版本号。

② 启用防破解时 iNode 既要满足前面所述的配套关系也必须高于此处限定的版本号。

(12) 系统参数配置检查

802.1x 和 Portal 认证场景下的防破解，均需要在单击“用户”→“接入策略管理”→“业务参数管理”→“系统配置”→“系统参数配置”命令后启用“客户端防破解”，如图 8-115 所示。



图 8-115　系统参数配置检查

(13) iNode 客户端配置检查

iNode 客户端侧需在属性设置里面选中“上传客户端版本号”复选框，否则 UAM 无法获取客户端版本导致认证失败，如图 8-116 所示。

说明：对于 802.1x 和 Portal 认证均需要勾选该项。

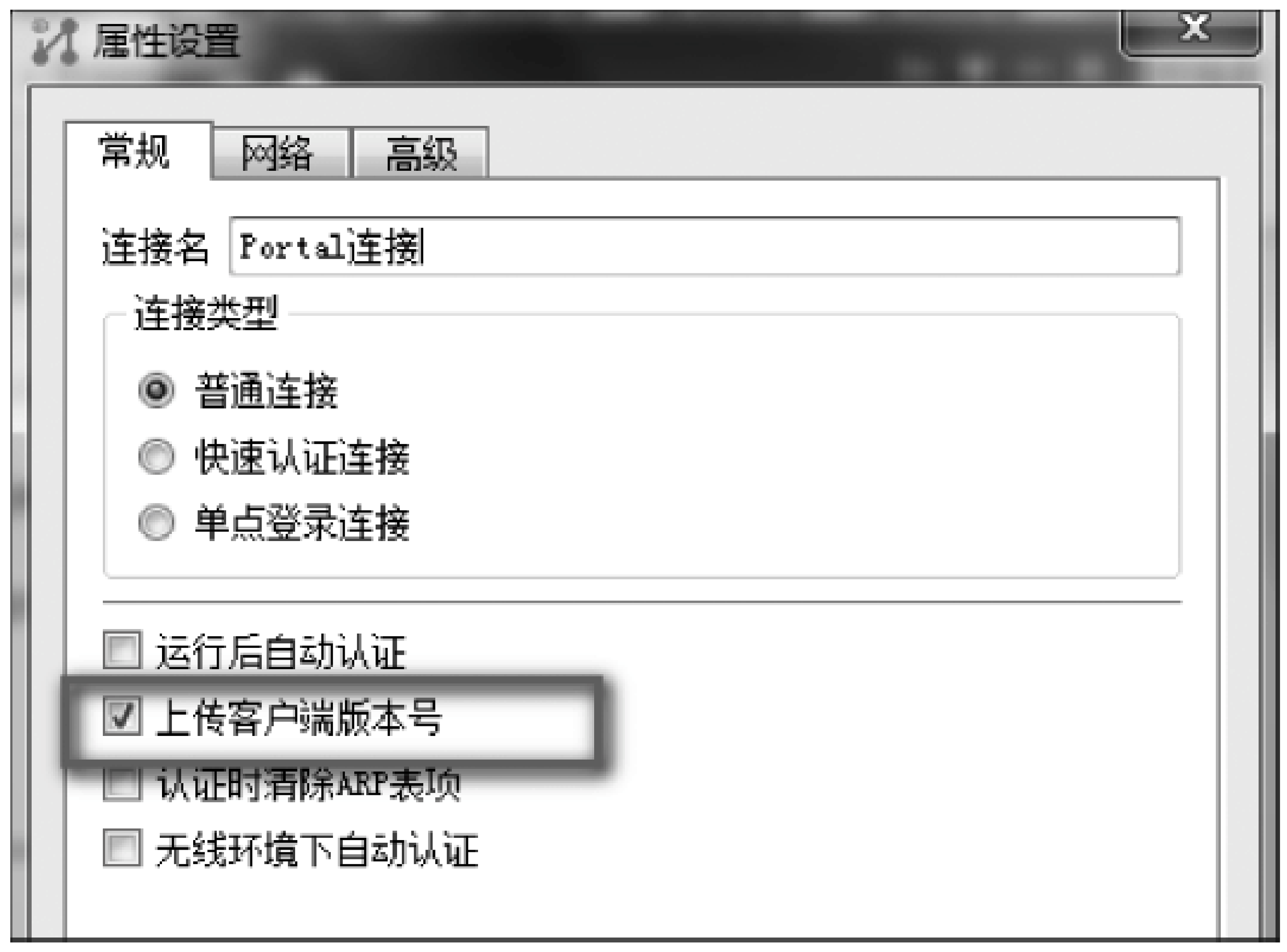
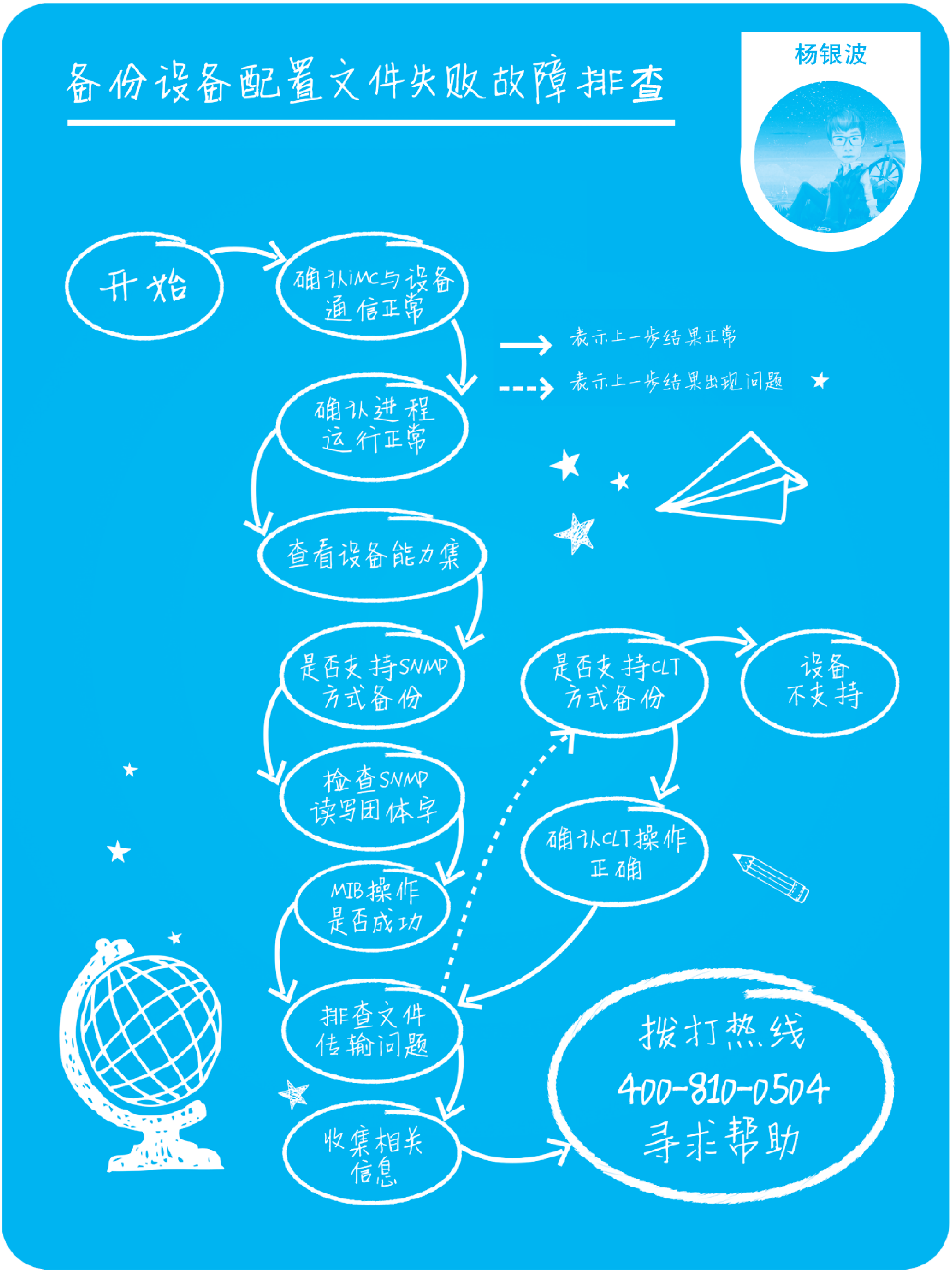


图 8-116　iNode 客户端配置检查


备份设备配置文件失败故障排查
杨银波
开始
确认iMC与设备通信正常
表示上一步结果正常
表示上一步结果出现问题
确认进程运行正常
查看设备能力集
是否支持SNMP方式备份
是否支持CLT方式备份
设备不支持
检查SNMP读写团体字
确认CLT操作正确
MIB操作是否成功
排查文件传输问题
收集相关信息
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC PLAT 提供了 iCC 智能配置中心功能来对设备的配置和软件进行管理，主要包括设备配置的手动\自动备份及下发，设备软件的手动\自动备份及下发等功能，能够大大减轻运维管理的工作量，高效安全地完成对网络中设备的管理和维护。本篇详细分析 iMC 进行设备配置备份时的具体实现原理和交互过程，并提供完整的故障排查思路，可供配置备份失败时参考。

（1）备份设备配置时 iMC 首先会尝试以 SNMP 方式去备份，具体为先向设备的 MIB 节点 hh3cCfgOperateRowStatus 写入整个过程需要下发的变量数，通常情况下备份设备配置的过程中会涉及 6 个变量，所以值一般为 6，如图 8-117 所示。

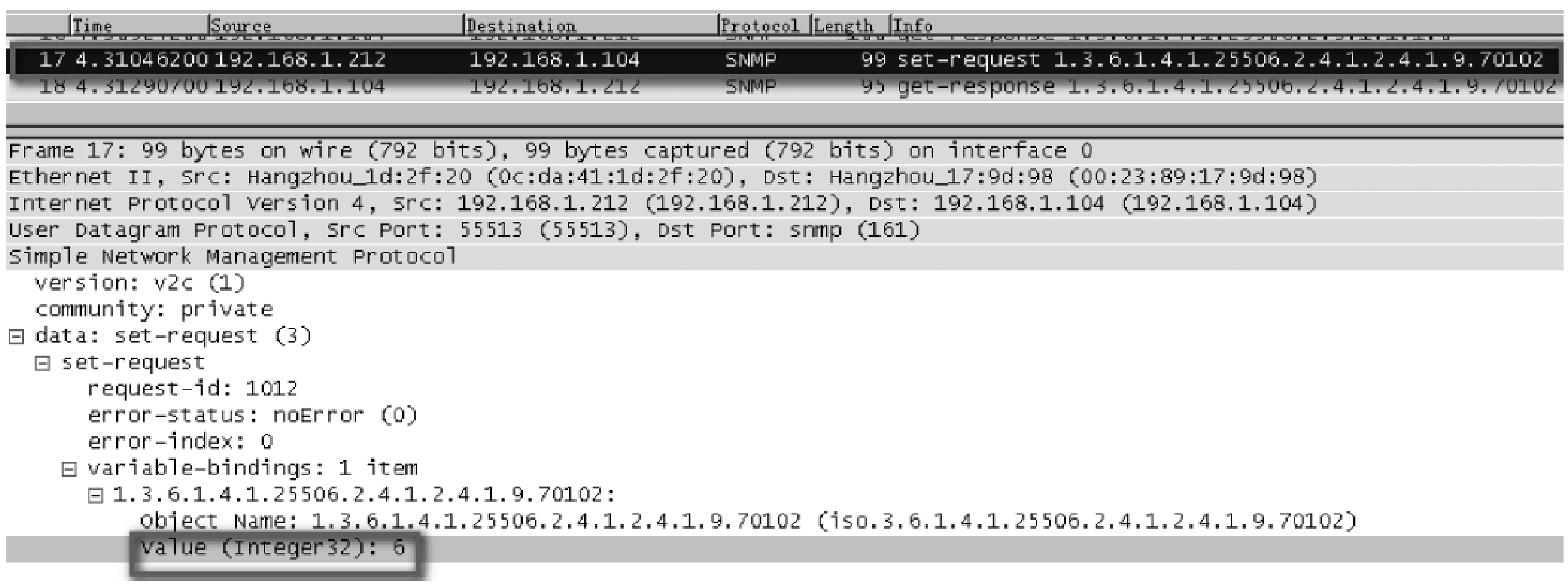


图 8-117　6 个变量

这一步操作没有问题后，iMC 会向设备的 hh3cCfgOperateType 节点下发此次的操作类型为备份配置，向 hh3cCfgOperateProtocol 节点下发传输配置文件所用的传输方式，向 hh3cCfgOperateFileName 节点下发要备份的文件名，向 hh3cCfgOperateServerAddress 节点下发接收备份的服务器地址，向 hh3cCfgOperateEndNotificationSwitch 节点下发操作结束标记等，如图 8-118 所示。

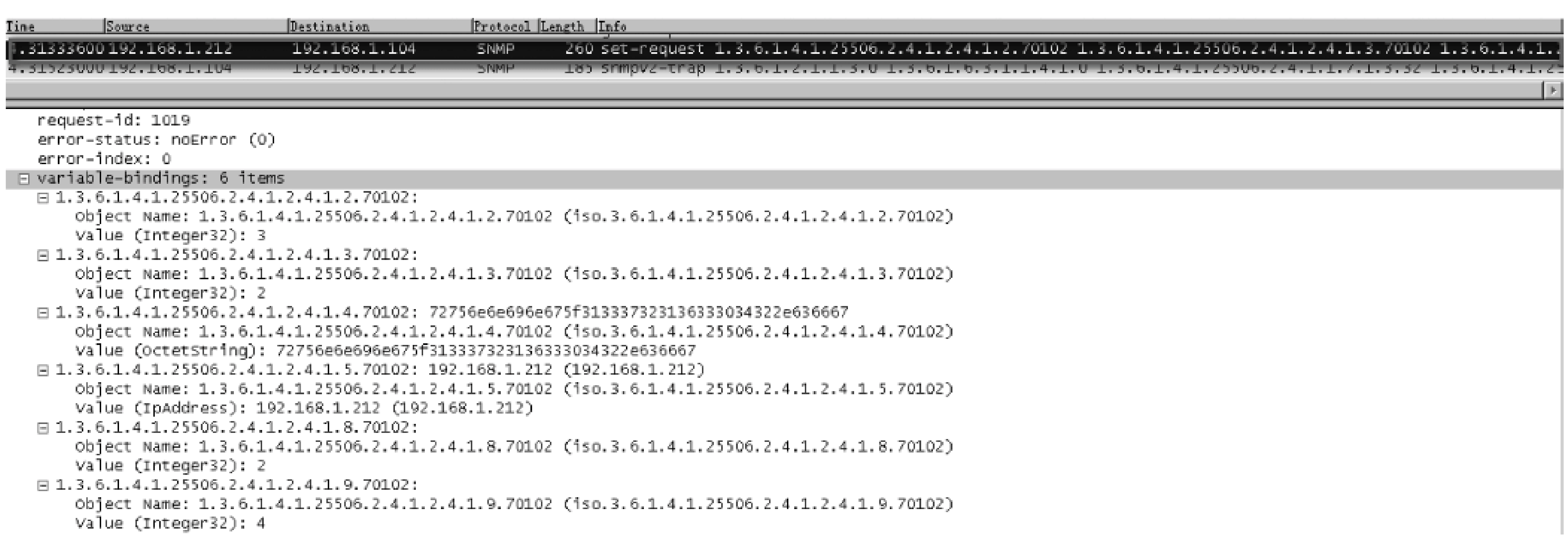


图 8-118　下发信息

只有保证以上操作没有问题,SNMP 方式才能备份成功。

(2) 如果 SNMP 方式备份失败,iMC 会再次尝试以 CLT 方式进行备份,具体为通过前期配置的设备登录方式(Telnet 或 SSH)先登录到设备,然后以执行命令的方式将配置文件传输过来。通过查看 iMC 配置备份的后台日志可以看到当 iMC 以 SNMP Set 方式向设备的 hh3cCfgOperateTable 表节点操作失败后,会以 Telnet 方式登录到设备执行 TFTP 命令传输文件,如图 8-119 所示。

```
2015-03-07 15:17:14.606 [ERROR (1)] [THREAD(2924)] [imcdm::decryptString()] Failed to decryptStringAes.
2015-03-07 15:17:14.646 [INFO (-1)] [THREAD(2924)] [CSnmpOper::iCommitOper] writecommunity is empty for snmpv1/2 set operation.->[192.168.1.104]
2015-03-07 15:17:14.646 [INFO (-1)] [THREAD(2924)] [CSnmpOper::iCommitOper] writecommunity is empty for snmpv1/2 set operation.->[192.168.1.104]
2015-03-07 15:17:14.646 [INFO (-1)] [THREAD(2924)] [CSnmpOper::iCommitOper] writecommunity is empty for snmpv1/2 set operation.->[192.168.1.104]
2015-03-07 15:17:14.646 [ERROR (-1)] [THREAD(2924)] [CH3CCfgManTableImp::doFileTransfer()] Failed to commit h3cCfgOperateTable

<H3C>delete /unreserved iccrunning.cfg
% Execution failure
<H3C>delete /unreserved iccrunning.zip
% Execution failure
<H3C>save iccrunning.cfg
The current configuration will be saved to cfa0:/iccrunning.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration cfa0:/iccrunning.cfg. Please wait...

Configuration is saved to cfa0 successfully.
<H3C>tftp 192.168.1.212 put iccrunning.cfg running_1372224512.cfg

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... /
  TFTP:     2805 bytes sent in 0 second(s).
  File uploaded successfully.

<H3C>display startup
 Current startup saved-configuration file: cfa0:/startup.cfg
 Next main startup saved-configuration file: cfa0:/startup.cfg
 Next backup startup saved-configuration file: NULL
<H3C>tftp 192.168.1.212 put cfa0:/startup.cfg startup_1372224612.cfg

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:     1842 bytes sent in 0 second(s).
  File uploaded successfully.
```

图 8-119 登录到设备执行 TFTP 命令传输文件

如果 SNMP 方式和 CLT 方式都操作失败后,则 iMC 会返回备份失败提示。

以上为 iMC 进行设备配置备份的处理流程,故出现问题时可按步顺序排查哪一步有问题。

2. 确认 iMC 与设备通信正常

第一步先确认备份时 iMC 是否和设备通信正常,由于备份时会用到 SNMP UDP 161,TELNET UDP 23 等端口,所以不只是要能 ping 通,最好测试一下这些端口是否能够正常连接。

3. 确认进程运行正常

请登录 iMC 服务器在部署监控代理中查看进程 imciccdm.exe 和 imccfgbakdm.exe 是否运行正常,并且如果经过后续排查也解决不了问题可以尝试重启这两进程,如图 8-120 所示。

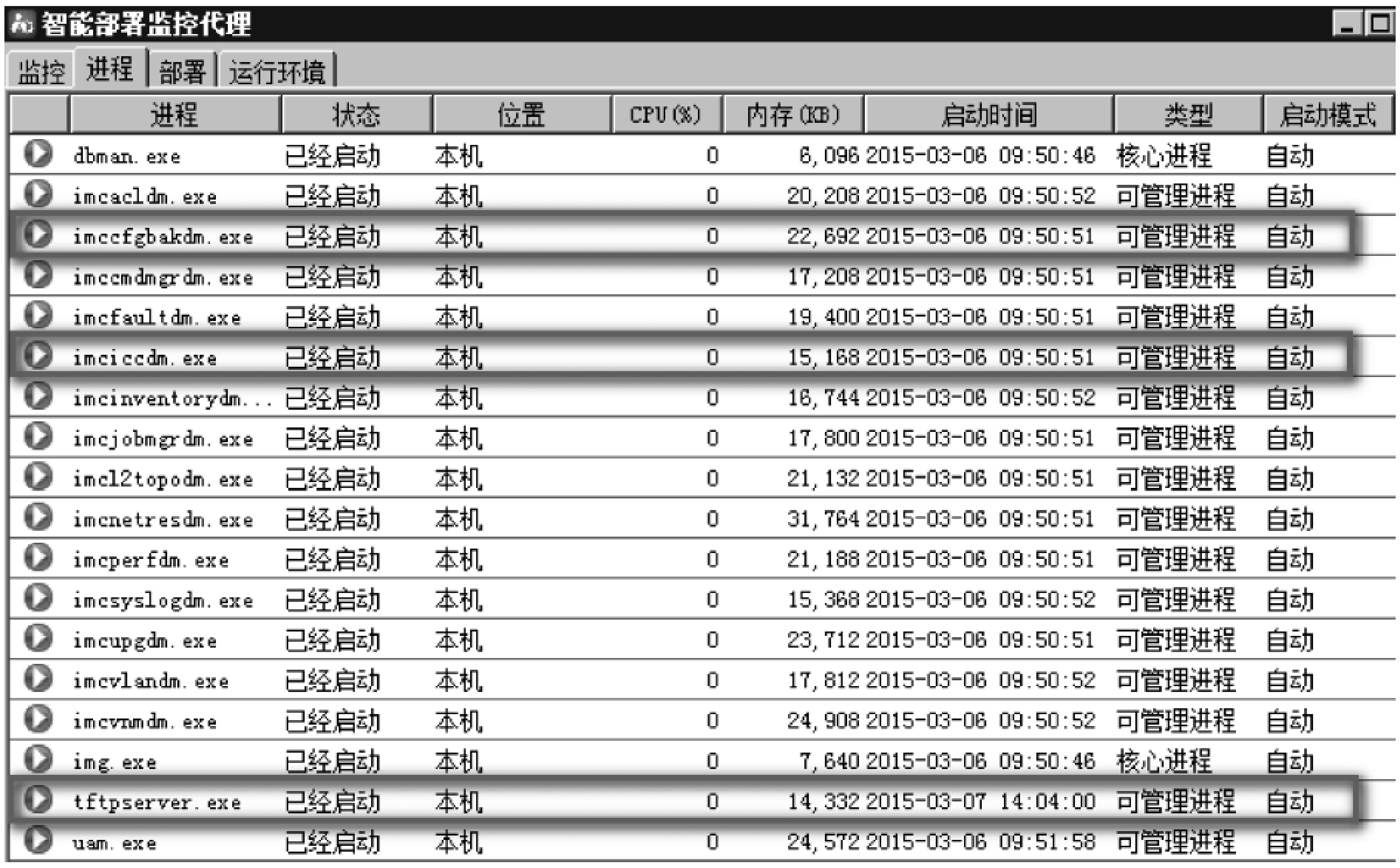
4. 查看设备能力集

在设备详细信息—设备能力集中查看一下本设备是否支持通过 SNMP 或 CLT 方式进行备份操作,这里列出了 4 种操作类型,2 种操作协议共 8 种情况的支持与否,以此来判断本次操作是否支持,如图 8-121 所示。

说明:某些版本的 iMC 可能没有这个界面,那么可忽略此步直接进行后续排查。

5. 是否支持 SNMP 方式备份

通过上步可以确认可否通过 SNMP 方式备份设备配置,如果设备支持,则可以进一步排查 SNMP 方面问题,如果不支持,则 iMC 会通过 CLT 方式备份设备配置,可排查 CLT 方面问题。



进程	状态	位置	CPU (%)	内存 (KB)	启动时间	类型	启动模式
dbman.exe	已经启动	本机	0	6,096	2015-03-06 09:50:46	核心进程	自动
imcacldm.exe	已经启动	本机	0	20,208	2015-03-06 09:50:52	可管理进程	自动
imccfgbakdm.exe	已经启动	本机	0	22,692	2015-03-06 09:50:51	可管理进程	自动
imccmdmgrdm.exe	已经启动	本机	0	17,208	2015-03-06 09:50:51	可管理进程	自动
imcfaultdm.exe	已经启动	本机	0	19,400	2015-03-06 09:50:51	可管理进程	自动
imciccdm.exe	已经启动	本机	0	15,168	2015-03-06 09:50:51	可管理进程	自动
imcinventorydm...	已经启动	本机	0	16,744	2015-03-06 09:50:52	可管理进程	自动
imcjobmgrdm.exe	已经启动	本机	0	17,800	2015-03-06 09:50:51	可管理进程	自动
imcl2topodm.exe	已经启动	本机	0	21,132	2015-03-06 09:50:51	可管理进程	自动
imcnetresdm.exe	已经启动	本机	0	31,764	2015-03-06 09:50:51	可管理进程	自动
imcperfdm.exe	已经启动	本机	0	21,188	2015-03-06 09:50:51	可管理进程	自动
imcsyslogdm.exe	已经启动	本机	0	15,368	2015-03-06 09:50:52	可管理进程	自动
imcupgdm.exe	已经启动	本机	0	23,712	2015-03-06 09:50:51	可管理进程	自动
imcvlandm.exe	已经启动	本机	0	17,812	2015-03-06 09:50:52	可管理进程	自动
imcvmdm.exe	已经启动	本机	0	24,908	2015-03-06 09:50:52	可管理进程	自动
img.exe	已经启动	本机	0	7,640	2015-03-06 09:50:46	核心进程	自动
tftpserver.exe	已经启动	本机	0	14,332	2015-03-07 14:04:00	可管理进程	自动
uam.exe	已经启动	本机	0	24,572	2015-03-06 09:51:58	可管理进程	自动

图 8-120　确认进程运行正常



设备名称	设备型号	操作类型	访问方式	支持TFTP	支持FTP	支持SFTP	支持SCP
H3C(192.168.1.104)	H3C MSR30-20	配置备份	CLI	是	是	是	否
H3C(192.168.1.104)	H3C MSR30-20	配置恢复	CLI	是	是	是	否
H3C(192.168.1.104)	H3C MSR30-20	软件备份	CLI	否	否	是	否
H3C(192.168.1.104)	H3C MSR30-20	软件升级	CLI	是	是	是	否
H3C(192.168.1.104)	H3C MSR30-20	配置备份	SNMP	是	是	否	否
H3C(192.168.1.104)	H3C MSR30-20	配置恢复	SNMP	是	是	否	否
H3C(192.168.1.104)	H3C MSR30-20	软件备份	SNMP	是	是	否	否
H3C(192.168.1.104)	H3C MSR30-20	软件升级	SNMP	是	是	否	否

图 8-121　2 种操作协议的支持与否

6. 检查 SNMP 读写团体字

iMC 备份设备配置时，需要进行 SNMP Set 操作，所以如果 iMC 和设备配置的读写团体字不一致就会导致备份失败，提示如图 8-122 所示错误。

出现此错误时，可在 iMC 单击“操作界面资源”→“批量操作”→“校验访问参数”命令后进行 SNMP 参数校验来确定 SNMP 参数的配置，如图 8-123 所示。

当校验结果为成功时则表示 iMC 和设备配置的 SNMP 读和读写团体字一致，如果返回错误则需要进行修改保证校验成功。

7. MIB 操作是否成功

如果 iMC 不支持备份此款设备(可在平台版本说明书中 iCC 部分查看)，或者设备 MIB 方面存在问题，可能会不存在配置备份操作需要 Set 的 MIB 节点，可以在抓包中看到 hh3cCfgOperateTable 中的节点返回值不存在的现象。则此设备无法通过 SNMP 方式进行配置备份操作。



图 8-122　SNMP Set 操作



图 8-123　SNMP 参数校验

8. 是否支持 CLT 方式备份

如果设备不支持 SNMP 方式备份或 SNMP 备份失败，请在设备能力集中查看是否支持 CLT 方式备份。

9. 设备不支持

如果设备不支持 SNMP 方式也不支持 CLT 方式备份，则此设备无法在 iMC 中进行备份操作。

10. 确认 CLT 操作正确

在设备详细信息页面可以看到配置的设备登录方式，请确保此处配置了登录方式，并且参数配置正确。可以在单击"资源"→"批量操作"→"检验访问参数"命令后，通过校验一下来确认。

如果登录方式配置正确，还可以打开 imccfgbakdm. txt 日志确认命令在设备上是否执行成功，如图 8-124 所示。

```
<H3C>display startup
 Current startup saved-configuration file: cfa0:/startup.cfg
 Next main startup saved-configuration file: cfa0:/startup.cfg
 Next backup startup saved-configuration file: NULL
<H3C>tftp 192.168.1.212 put cfa0:/startup.cfg startup_1372224612.cfg

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:      1842 bytes sent in 0 second(s).
  File uploaded successfully.
```

图 8-124　用 imccfgbakdm. txt 日志确认命令执行情况

11. 排查文件传输问题

如果备份操 SNMP Set 或 CLT 方式成功触发了备份操作，但是备份失败，则有可能是文件传输过程中有问题。可在 iMC 页面单击“业务”→“设备配置管理”→“选项”→“文件传输方式”命令后查看设置的文件传输方式（默认为 TFTP 方式，iMC 本身包含一个 imctftpdm. exe 进程作为 TFTP 服务器端），如图 8-125 所示。



图 8-125　查看设置的文件传输方式

如果 imctftpdm. exe 进程运行异常或设备配置的 TFTP 源地址有问题等，即会造成 TFTP 传输错误，如图 8-126 所示。

12. 收集相关信息

如果以上步骤排查完都不能解决问题，请反馈以下信息联系 H3C 售后支持热线处理。

① 设备型号版本，运行配置。

② iMC 版本。

③ 配置备份过程中 iMC 服务器上的抓包。

④ IMC 的后台日志，收集方法为先在 iMC 安装目录 imc\server\conf\qvdm. conf 文件中将 LogLevel＝INFO 改为 LogLevel＝DEBUG，重启 imciccdm. exe 和 imccfgbakdm. exe 进程，然后进行备份操作，失败后反馈 iMC 安装目录 imc\server\conf\log\目录中的 imciccdm. txt 和 imccfgbakdm. txt 文件。

业务 > 设备配置一览表 > H3C(192.168.1.104) > 备份配置文件结果

备份配置文件结果

手工备份设备结束。共备份"1"个设备，其中：备份成功"0"个设备，备份失败"1"个设备。

设备名称	设备型号	配置文件类型	时间	结果	配置文件名称	详细步骤
			2015-03-07 13:50:51	✓ 共备份"0"个配置文件，其中：启动配置文件"0"个，运行配置文件"0"个。		
H3C(192.168.1.104)	H3C MSR30-20	运行	2015-03-07 13:50:50	✕ TFTP Server未启动。	--	
H3C(192.168.1.104)	H3C MSR30-20	启动	2015-03-07 13:50:50	✕ TFTP Server未启动。	--	
			2015-03-07 13:50:45	✓ 备份配置文件开始。		

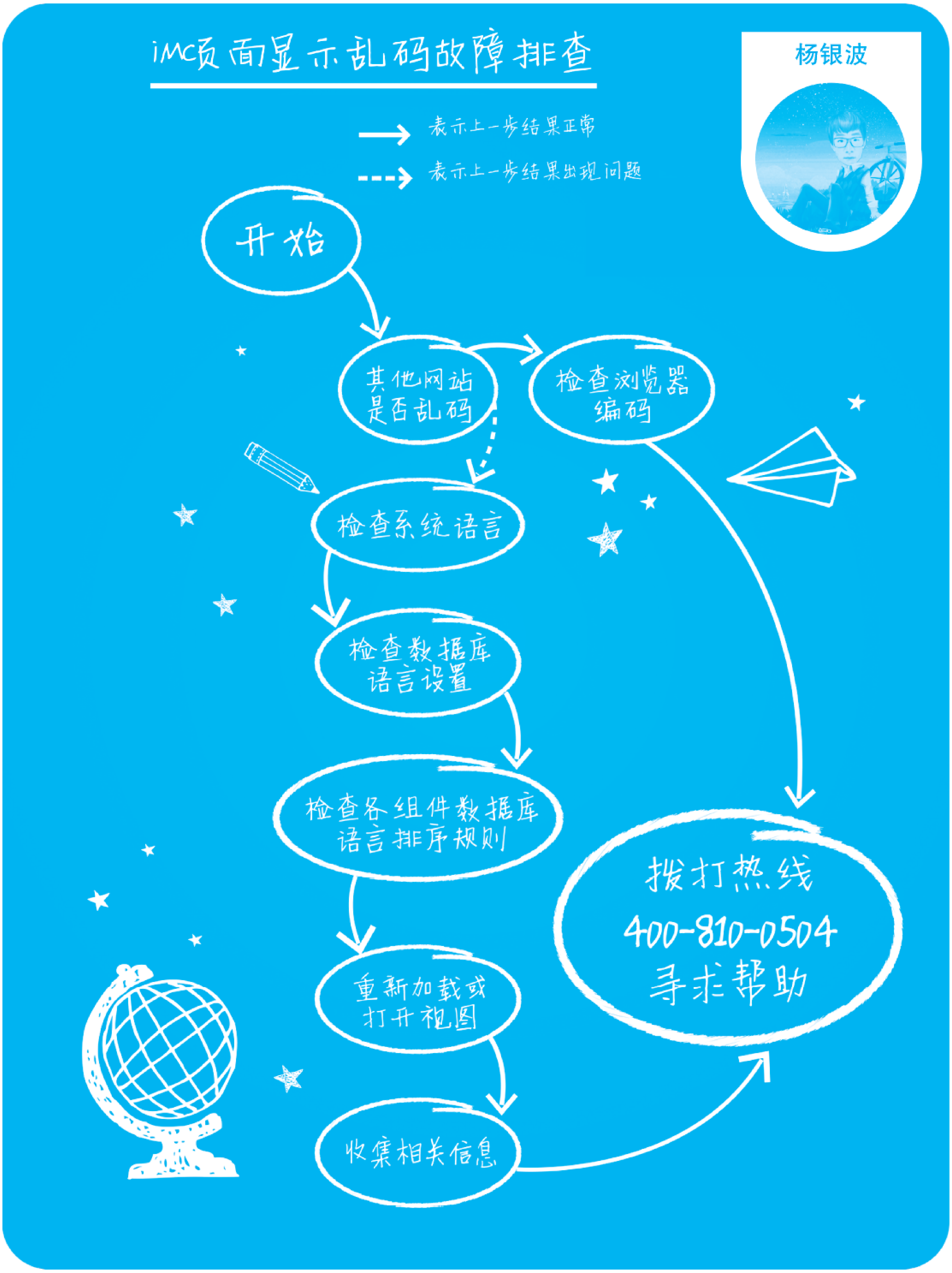
业务 > 设备配置一览表 > H3C(192.168.1.104) > 备份配置文件结果

备份配置文件结果

手工备份设备结束。共备份"1"个设备，其中：备份成功"0"个设备，备份失败"1"个设备。

设备名称	设备型号	配置文件类型	时间	结果	配置文件名称	详细步骤
			2015-03-07 14:08:19	✓ 共备份"0"个配置文件，其中：启动配置文件"0"个，运行配置文件"0"个。		
H3C(192.168.1.104)	H3C MSR30-20	启动	2015-03-07 14:08:18	✕ TFTP方式从设备传输配置文件到iMC服务器失败。	--	
H3C(192.168.1.104)	H3C MSR30-20	运行	2015-03-07 14:08:18	✕ TFTP方式从设备传输配置文件到iMC服务器失败。	--	
			2015-03-07 14:04:46	✓ 备份配置文件开始。		

图 8-126　TFTP 传输错误


iMC页面显示乱码故障排查
杨银波
表示上一步结果正常
表示上一步结果出现问题
开始
其他网站是否乱码
检查浏览器编码
检查系统语言
检查数据库语言设置
检查各组件数据库语言排序规则
重新加载或打开视图
收集相关信息
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC 为 B/S 架构，客户端只需要安装浏览器就可以轻松管理 iMC，iMC 目前只支持简体中文和英文两种语言。并且 iMC 基于操作系统和数据库运行，所以页面内容的显示也会受到系统和数据库语言环境的影响。本篇详细讲解在 iMC 页面出现乱码问题时的故障排查思路。

2. 其他网站是否乱码

如果此浏览器打开其他和 iMC 语言相同的网页也会出现乱码，则有可能是浏览器编码设置问题，如果不乱码则可排除编码问题，进行后续步骤排查。

3. 检查浏览器编码

以 IE 浏览器为例，可在浏览器中单击“命令栏”→“页面”→“编码”命令后进行设置，如图 8-127 所示。



图 8-127 检查浏览器编码

4. 检查系统语言

如果其他网页显示正常或浏览器编码设置没有问题，则需要确认操作系统显示语言为简体中文，Windows 系统可在单击“控制面板”→“区域和语言”命令后选择“键盘和语言”选项卡，会看到当前系统显示语言语种，如图 8-128 所示。

如果这里显示的不是中文(简体)并且下拉框中也无法选择时，就需要安装语言包，在此页单击“安装”→“卸载语言”命令后会弹出选择文件页面，选择好之前下载到的语言包后单击“确定”按钮，即可完成语言包的安装。目前微软官网也提供直接运行安装的.exe 格式语言包，直接双击即可完成安装，如图 8-129 所示。

完成后就可看到此时显示语言下拉框已经有了可选的语言了，选择好后单击“确定”按钮即可完成显示语言设置，如图 8-130 所示。

完成后需要重启系统以使设置生效。



图 8-128　系统显示语言语种

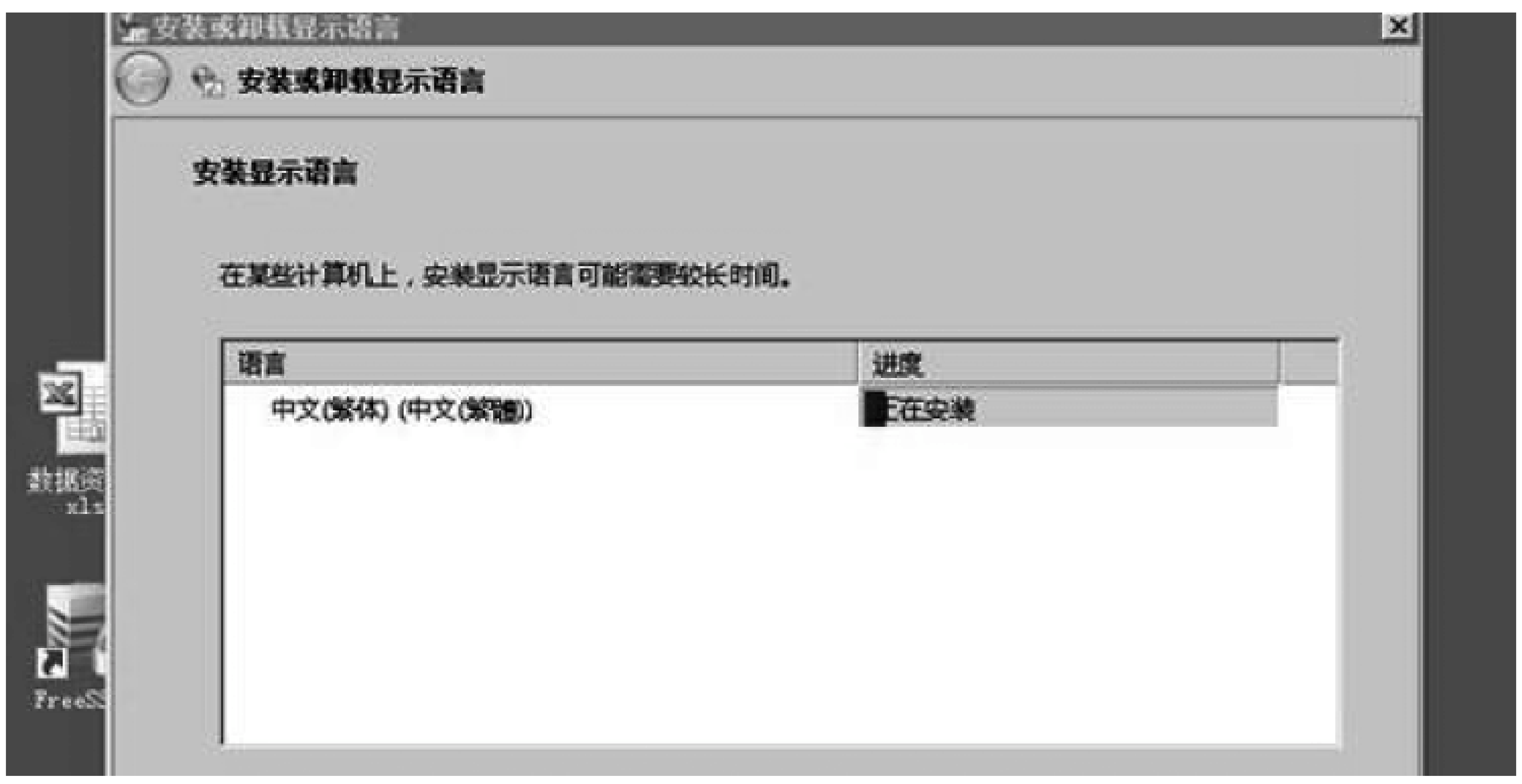


图 8-129　完成安装



图 8-130　完成显示语言设置

Linux 系统可执行命令 echo ＄LANG 来确认系统语言设置，如果执行结果为 zh_CN. UTF-8 则证明设置的是中文环境，如果不是则需要以 root 用户登录到 iMC 服务器并打开/root/目录下的. porfile 文件，并在其中添加 LANG＝zh_CN. UTF-8，export LANG 命令，添加完成后保存退出，如图 8-131 所示。

添加后可执行命令 source . profile 或重启系统使之生效。

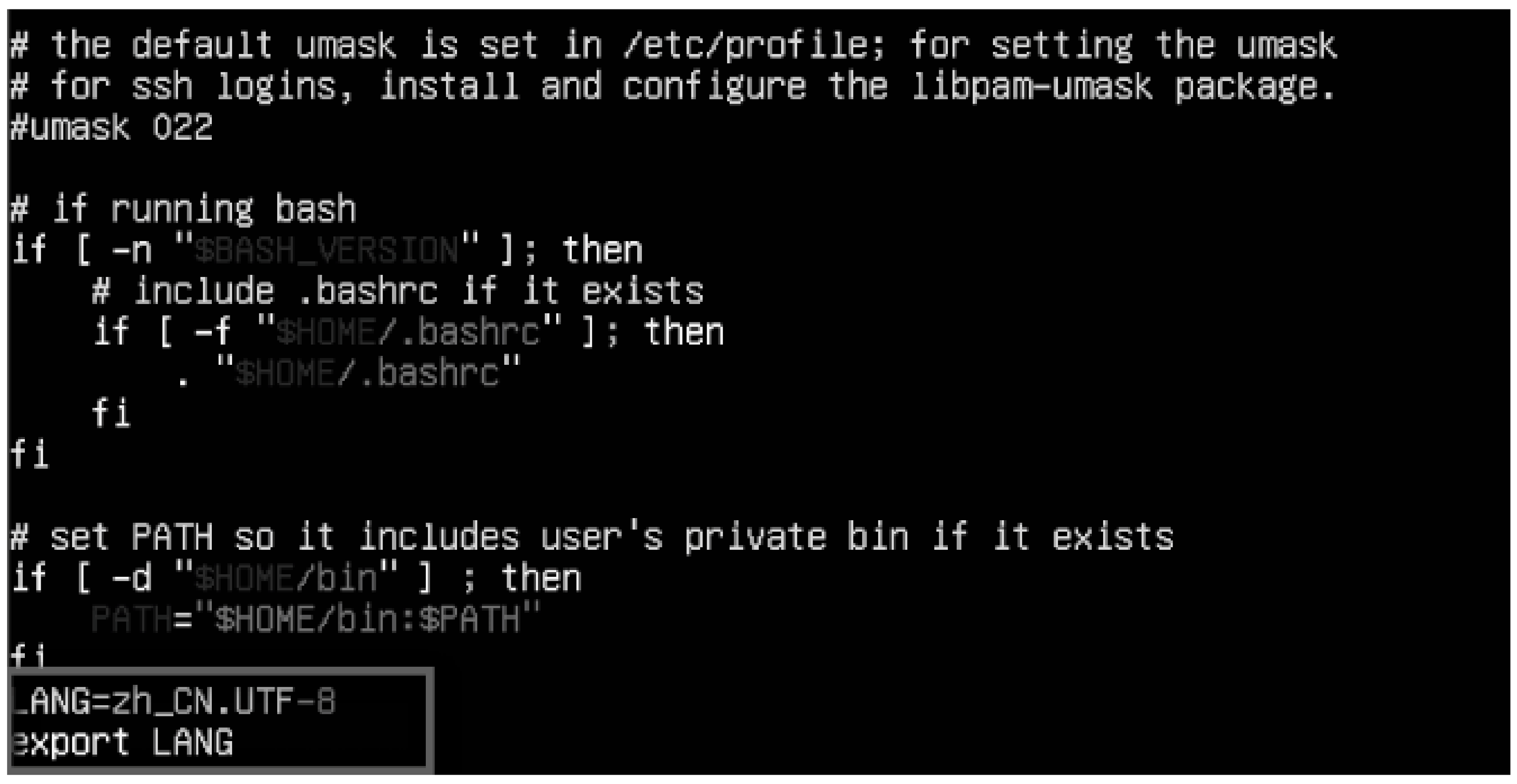


图 8-131　用 echo ＄LANG 命令来确认系统语言设置

5. 检查数据库语言设置

Windows 系统时可登录数据库客户端，连接 iMC 所使用的数据库实例，右击选择“属性”命令，查看“常规”中语言是否为中文(简体，中国)，如图 8-132 所示。



图 8-132　查看“常规”中语言是否为中文

查看“高级”中默认语言是否为 Simplified Chinese，如图 8-133 所示。



图 8-133　查看“高级”中默认语言是否为 Simplified Chinese

Linux 系统时需要保证在安装 Oracle 数据库过程中设置的字符编码格式为 Simple Chinese ZHS16GBK，如果设置不对的话则需要重新安装数据库。

6. 检查各组件数据库语言排序规则

在 iMC 中每个组件都有其自己的数据库，如果其他页面都显示正常，只有关于此组件的

页面乱码，则有可能只是该组件的数据库语言设置有问题。比如经常会出现性能监控实例乱码，这时就需要确认性能数据库 perf_db 的语言排序规则。确认其所使用的数据库语言排序规则为 Chinese_PRC_CI_AS，选择 perf_db 右击后选择"属性"命令，在常规中查看排序规则，如图 8-134 所示。



图 8-134 检查各组件数据库语言排序规则

如果更改不成功的话可重启数据库服务然后更改，须确保每个数据库都使用此种排序规则，使用其他排序规则的组件在其显示页面都可能会出现乱码。

7. 重新加载或打开视图

到这里的话基本上乱码问题已经排查得差不多了，重新打开 iMC 页面应该会恢复正常。特别注意的是如果乱码出现在性能监控实例和告警描述时，那么之前的告警乱码是无法修改的，新产生的告警则显示正常。性能监视实例的可以通过重新获取实例来解决，操作步骤为重新添加已监控的这些实例，这里需要注意的是因为这些实例已经添加了，默认情况下是选择不了再次添加的，需要先在增加监视页面右上角勾选"重新获取实例"，选择好实例之后单击"确定"按钮即可，如图 8-135 所示。

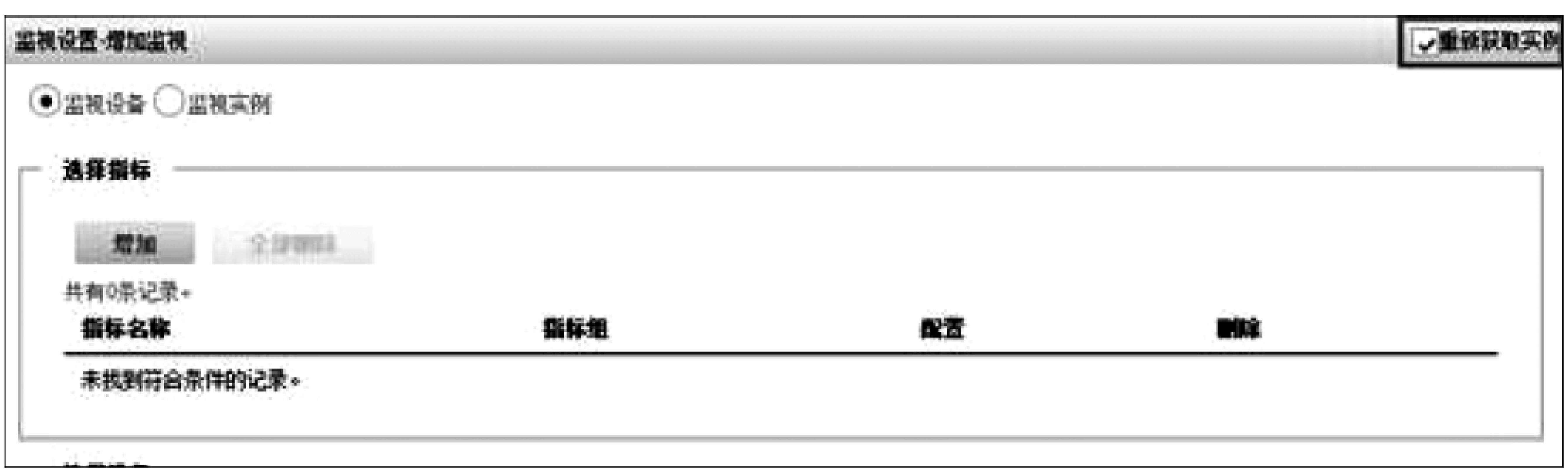


图 8-135 重新加载或打开视图

8. 收集相关信息

如果以上步骤排查完之后还是不能解决页面乱码问题，请反馈相关信息联系 H3C 售后技术支持热线 400-810-0504 解决。

iMC页面响应慢故障排查

杨银波





1. 开始

iMC 智能管理中心采用 B/S 架构设计，管理员对 iMC 的所有操作都可以在浏览器页面完成。所以操作页面的响应速度就直接影响管理员的工作效率。本篇详细分析各种情况导致 iMC 页面响应慢的现象，并提供排查思路，供现场故障时参考。

2. 是否所有页面都慢

为提高响应速率，iMC 内部采用模块化设计，相应模块独立到各自数据库中读取数据给前台显示，所以首先请判断是所有页面都慢还是只有个别页面慢。可登录 iMC 页面对资源、用户、业务、告警等所有页面逐个进行单击测试，并记录异常页面是否存在共性。

说明：如果单击某个页面报错并提示"返回首页"，可能是系统后台正在进行数据同步等比较繁忙，可以稍后单击尝试。

3. 检查服务器负载情况

如果 iMC 的所有页面都响应缓慢，有可能就是服务器本身的性能不足导致，请着重检查服务器 CPU 利用率，内存利用率，网速情况，磁盘 I/O 性能，如图 8-136 所示。

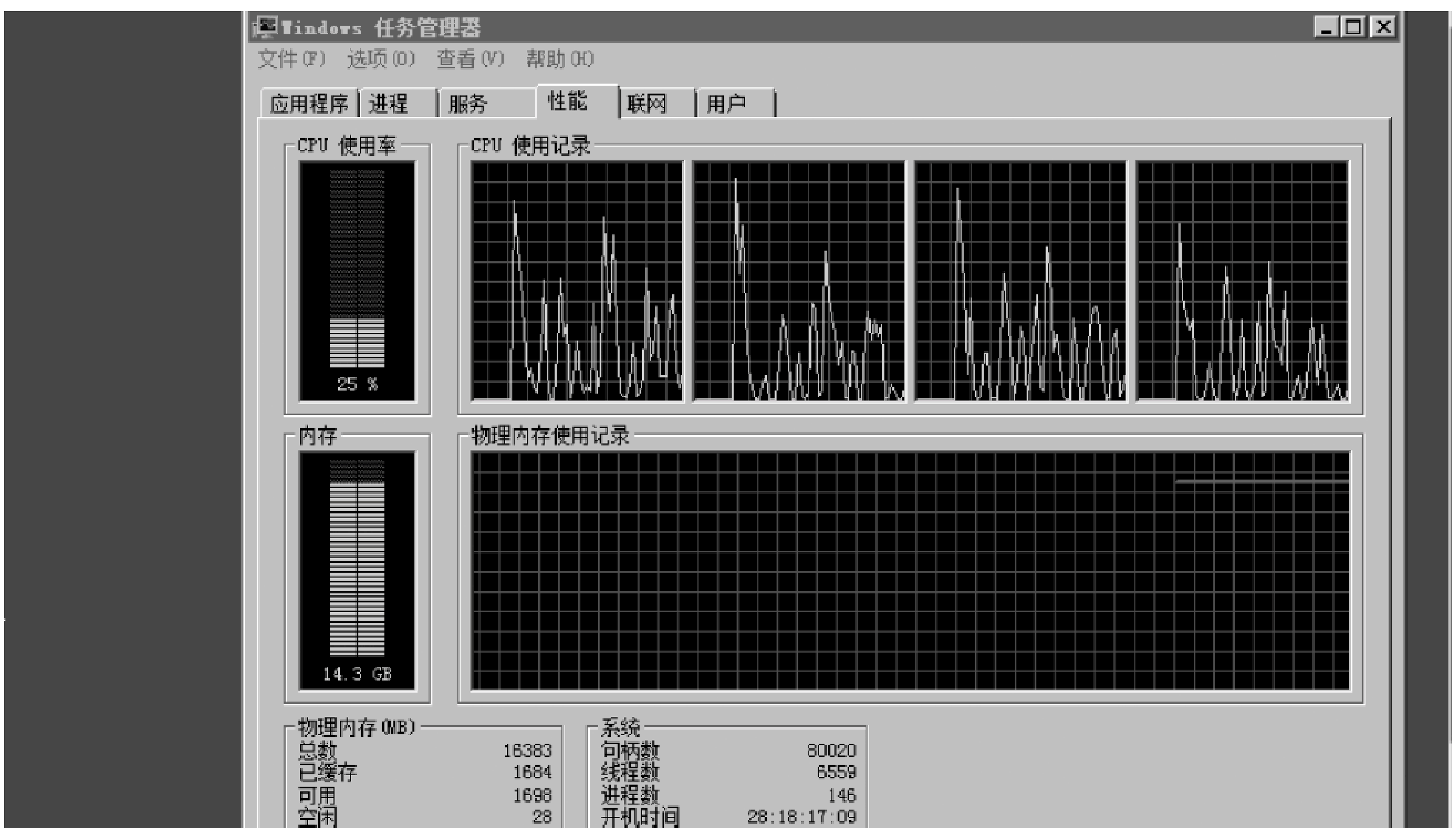


图 8-136 检查服务器负载情况

4. 硬件规格是否符合要求

如果 iMC 平稳运行中服务器的 CPU，内存等利用率都非常高，就说明目前的硬件规格不满足业务量的需求。iMC 在安装部署时对服务器的性能有严格的要求，并且给出了对应的标准。详细内容请参考《iMC 安装部署硬件指导》。

5. 硬件扩容

对于不符合《iMC 安装部署硬件指导》要求的局点，请协调客户对服务器进行扩容。性能

较差的服务器不但无法发挥 iMC 的最大性能而且还可能会造成各种异常现象。

6. 限制数据库内存

如果服务器内存已经达到了《iMC 安装部署硬件指导》中的要求，但是资源管理器中还是显示内存利用率非常大，有可能就是 SQL Server 数据库导致的。由于 SQL Server 对内存的使用规则是占用后就不会自动释放，所以数据库运行久了会导致数据库占用的内存越来越大。这时可以通过限制数据库最大内存来对其进行限制。一般建议限制为实际服务器内存的一半。限制方法有两种，分别如下。

① 在 iMC 服务器上命令行进入 iMC 安装目录 Imc\client\bin\，执行 setsqlservermaxmem.bat -server ** -saPwd ** -maxMem *** 命令来设置，具体执行方法如图 8-137 所示。

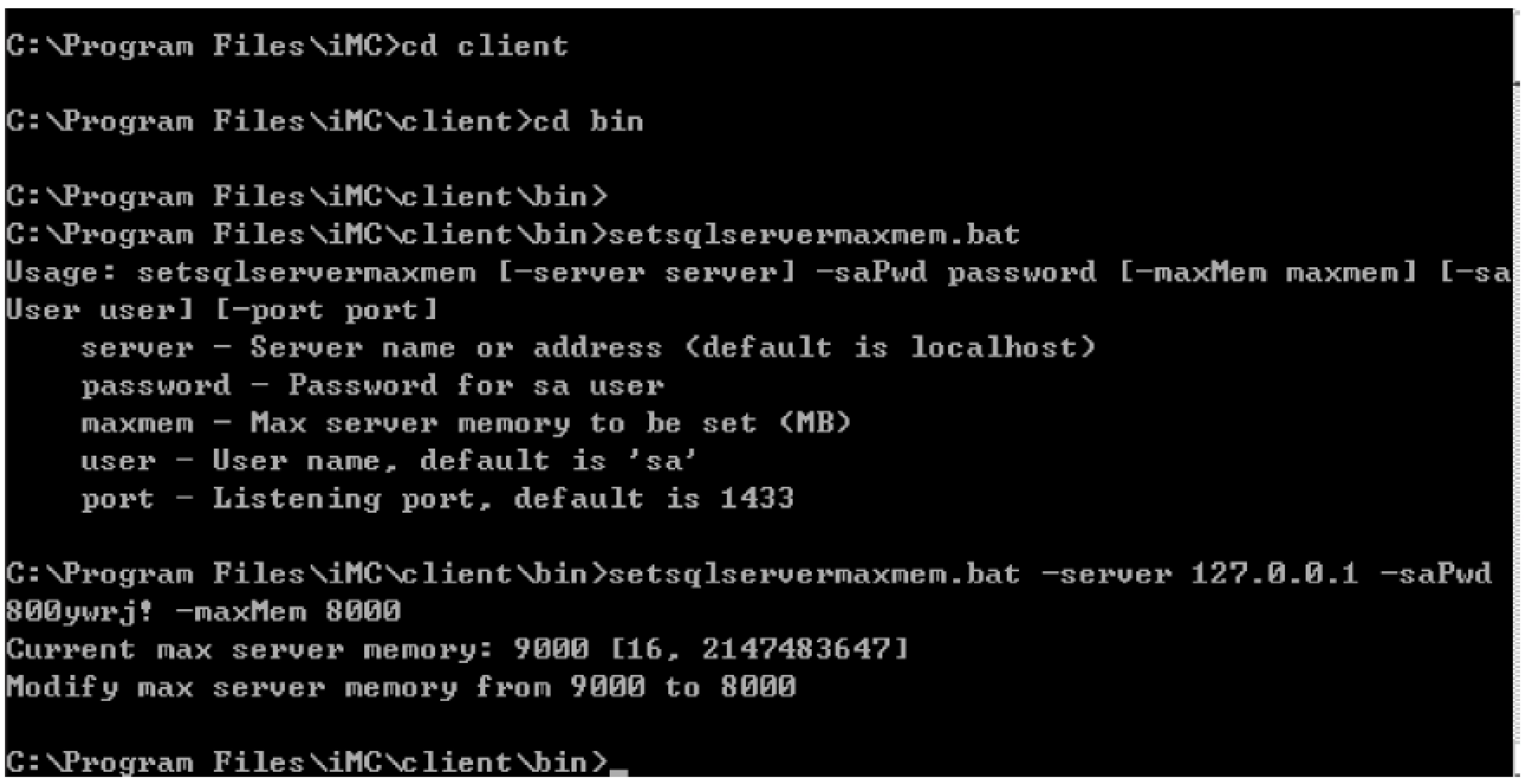


图 8-137 限制方法一

② 如果觉得执行上述命令麻烦，可以打开数据库客户端 SQL Server Management Studio，连接数据库实例。在实例名上单击右键选择“属性”命令后选择内存，在“最大服务器内存”处输入要设置的最大数即可，如图 8-138 所示。

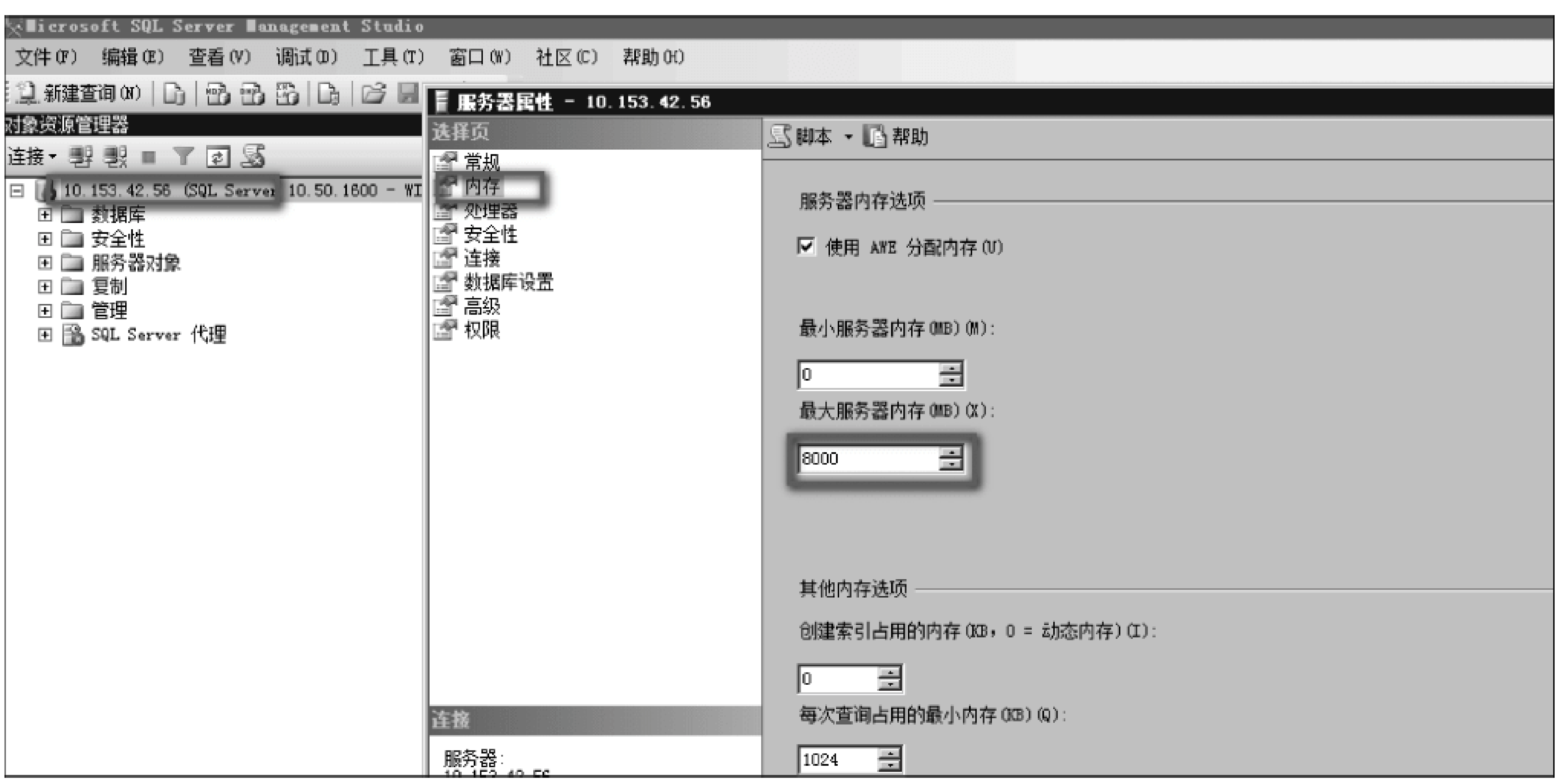


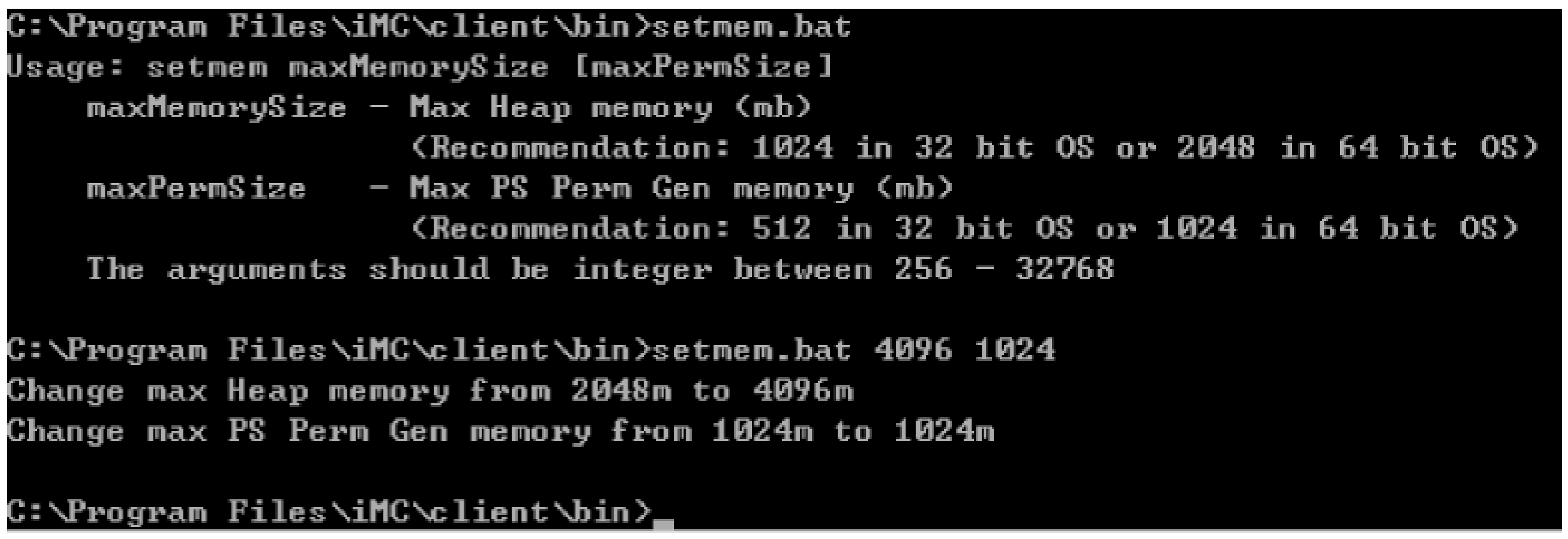
图 8-138 限制方法二

说明：这两种方法设置完成后都需要重新启动数据库服务使之生效。

7. 扩大前台内存

iMC 分为前台和后台两部分，前台的主程序就是 jserver.exe 进程。为了平衡性能 iMC 预先已经限制了前台进程可以使用的内存上限。所以如果服务器本身的内存利用率已经不高了，但是页面还是响应缓慢，可以将前台进程可用的内存限额扩大一点。扩大方法如下。

在 iMC 服务器中打开命令行窗口，并进入 iMC 安装目录 Imc\client\bin\目录，执行 setmem.bat ＄maxMemorySize ＄maxPermSize，具体如图 8-139 所示。



```
C:\Program Files\iMC\client\bin>setmem.bat
Usage: setmem maxMemorySize [maxPermSize]
    maxMemorySize - Max Heap memory (mb)
                    (Recommendation: 1024 in 32 bit OS or 2048 in 64 bit OS)
    maxPermSize   - Max PS Perm Gen memory (mb)
                    (Recommendation: 512 in 32 bit OS or 1024 in 64 bit OS)
    The arguments should be integer between 256 - 32768

C:\Program Files\iMC\client\bin>setmem.bat 4096 1024
Change max Heap memory from 2048m to 4096m
Change max PS Perm Gen memory from 1024m to 1024m

C:\Program Files\iMC\client\bin>_
```

图 8-139　扩大前台内存

说明：

① 如果系统是 32 位的，maxMemorySize /maxPermSize 设置不应超过 1024/512，否则会导致 jserver.exe 进程无法启动。

② 设置完成后必须重启 jserver.exe 进程使之生效。

8. 是否只有设备详细信息页面慢

单击设备标签进入设备详细信息页面时 iMC 会通过 SNMP 读取一下设备的最新信息，所以如果 SNMP 参数配置错误，就会导致这个页面（通常是右侧那几栏）显示缓慢。

9. 修改 SNMP 参数一致

在设备详细信息页面单击"配置"→"修改 SNMP 参数"填写 SNMP 读写团体字，完成后单击"测试"按钮确保测试成功，如图 8-140 所示。

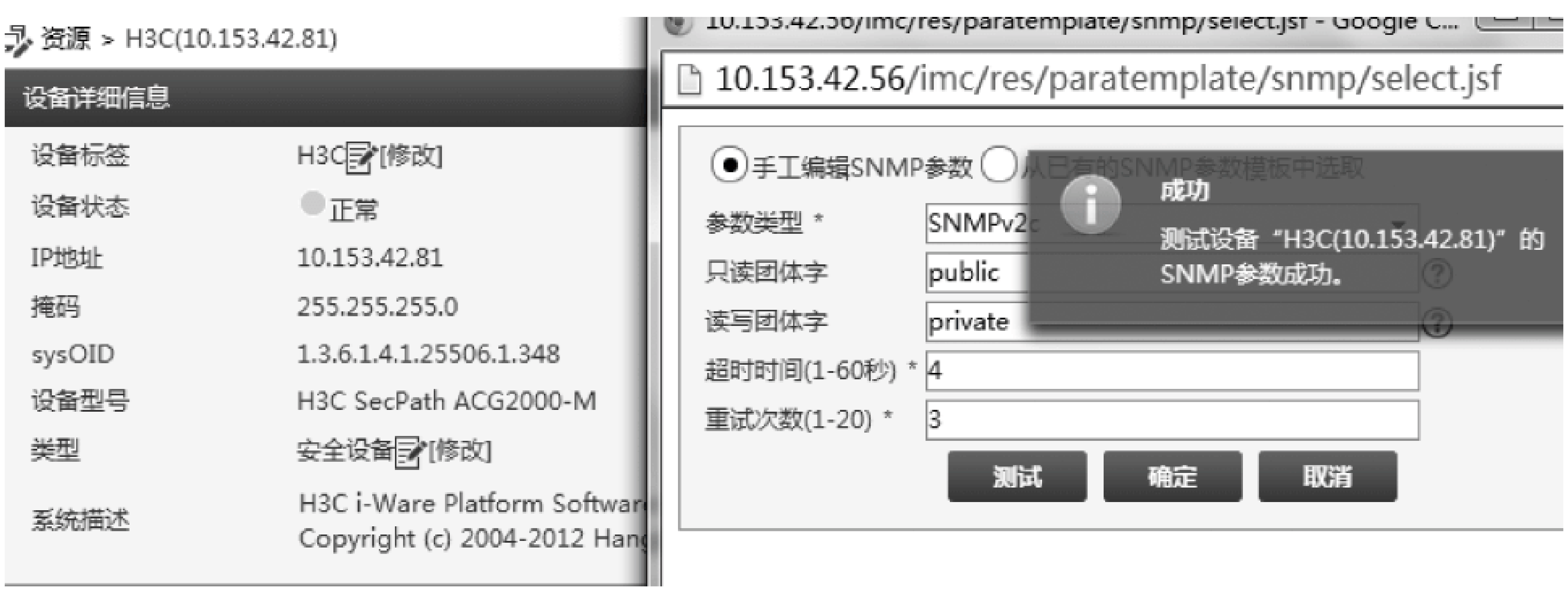


图 8-140　有"测试"按钮情况

如果 iMC 版本较老，可能没有"测试"按钮，此时可以在单击"资源"→"批量操作"→"校验访问参数"命令后，校验一下 iMC 和设备的 SNMP 参数是否一致，如图 8-141 所示。



图 8-141　无"测试"按钮情况

10. 收集信息

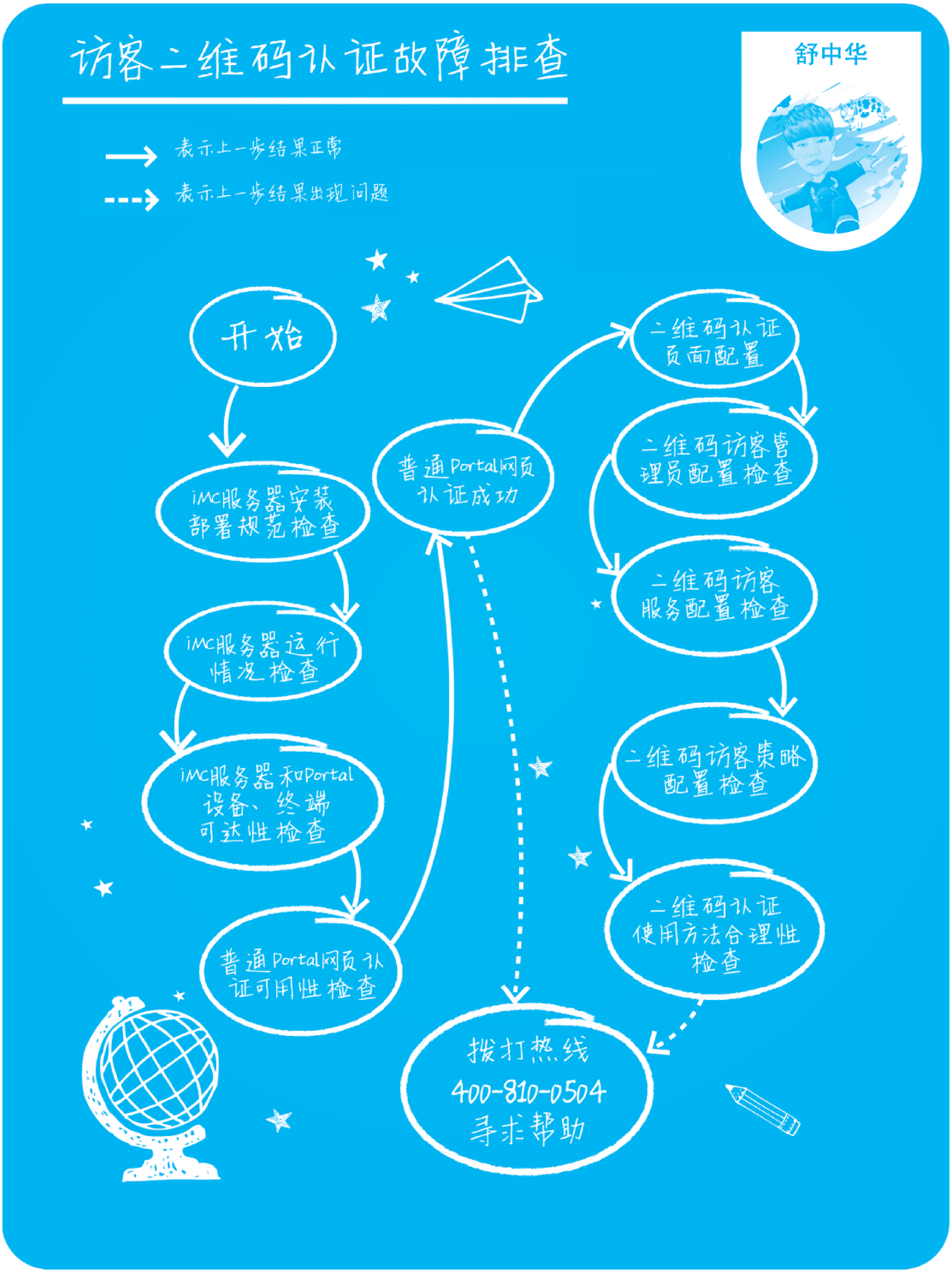
如果以上步骤都无法解决页面慢问题，请收集相关信息反馈华三售后技术支持中心处理。需要的信息如下。

① 响应缓慢的页面截图，并说明是哪些页面或进行哪些操作时响应缓慢。

② iMC 前台日志文件 imc\client\log\imcforeground.log。

③ iMC 版本。

拨打热线 400-810-0504 寻求帮助。


访客二维码认证故障排查
舒中华
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和Portal设备、终端可达性检查
普通Portal网页认证可用性检查
普通Portal网页认证成功
二维码认证页面配置
二维码访客管理员配置检查
二维码访客服务配置检查
二维码访客策略配置检查
二维码认证使用方法合理性检查
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC 访客二维码认证方案将新兴的二维码技术融入访客认证的流程中，极大地方便了智能终端接入 Wi-Fi 网络。扫描二维码审批功能与 Portal 认证相结合，实现了自动预注册、扫描二维码审批、自动认证的快速认证。扫描二维码认证功能与 Portal 认证相结合，实现了一键注册、扫描二维码即可自动认证的快速认证。

iMC 访客二维码认证方案排错定位思路：首先检查服务器软硬件及性能是否满足当前认证需要，然后需要确保普通 Portal 网页能正常上线，相应做 iMC 服务器的检查、访客服务、访客策略、访客管理员、访客系统参数配置的检查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击"开始"→"智能部署监控代理"命令，选择"部署"标签，检查"用户接入管理"功能模块及"Portal 服务器"功能模块是否已经部署，如图 8-142 所示。



图 8-142 各功能模块部署情况

说明：访客二维码认证方案基于 Portal 网页认证，故必须安装部署 EIA 功能组件及 Portal 服务器。

(2) iMC 服务器运行情况检查

① 打开部署监控代理，查看 uam.exe、portalserver、uamjob 进程是否正常启动。由于二维码认证基于网页 Portal 认证，故必须确认 Portal 服务器上的 jserver/webserver 进程正常启动，如图 8-143 所示。

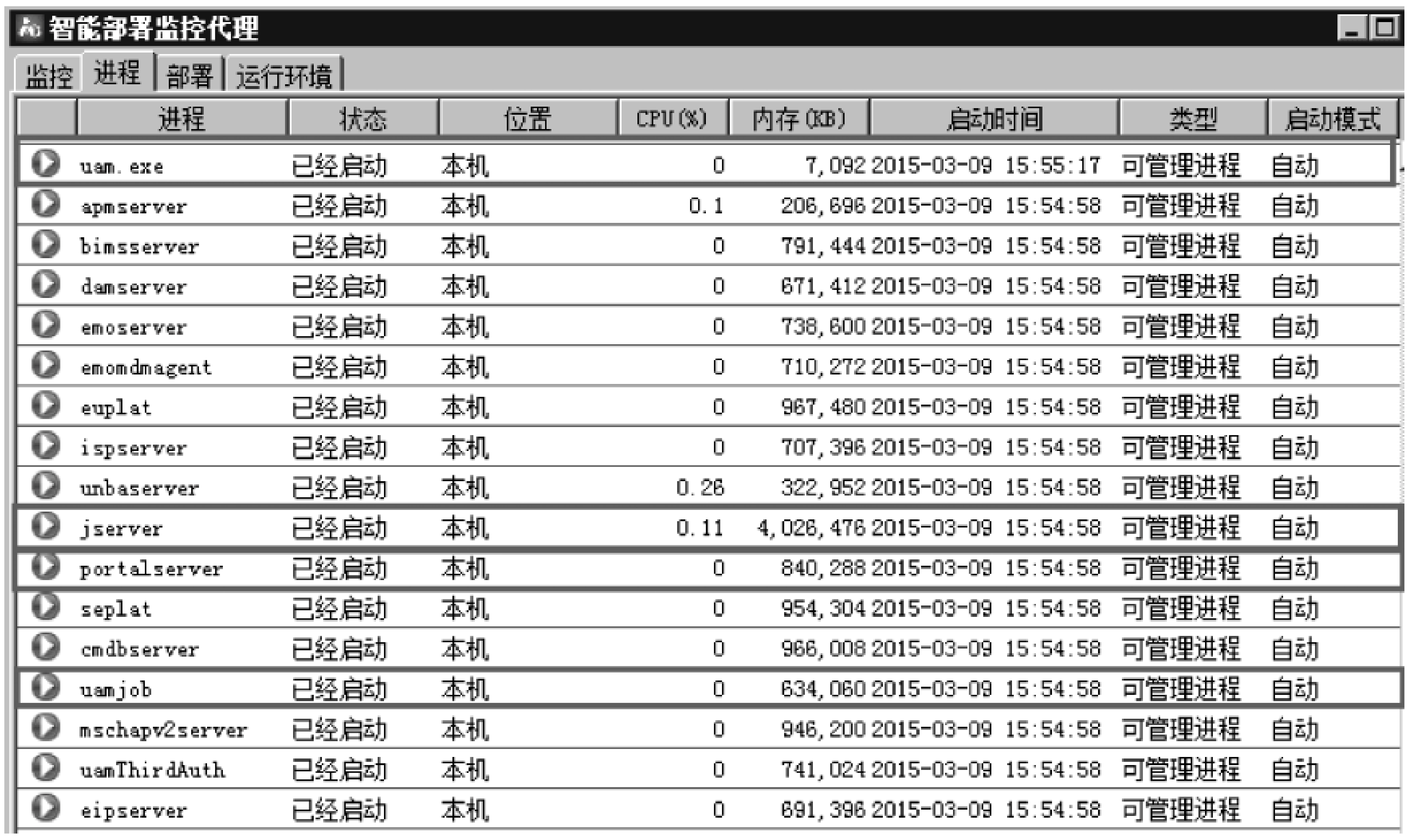


图 8-143　各进程正常启动情况

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) JServer 是 Portal 组件集中式部署时所需关注的进程；WebServer 为 Portal 组件分布式部署时，在从机上需要确认的进程。

② 检查服务器 1812、1813、50100、50200 UDP 端口是否被 uam 相关进程所监听，如图 8-144 所示。

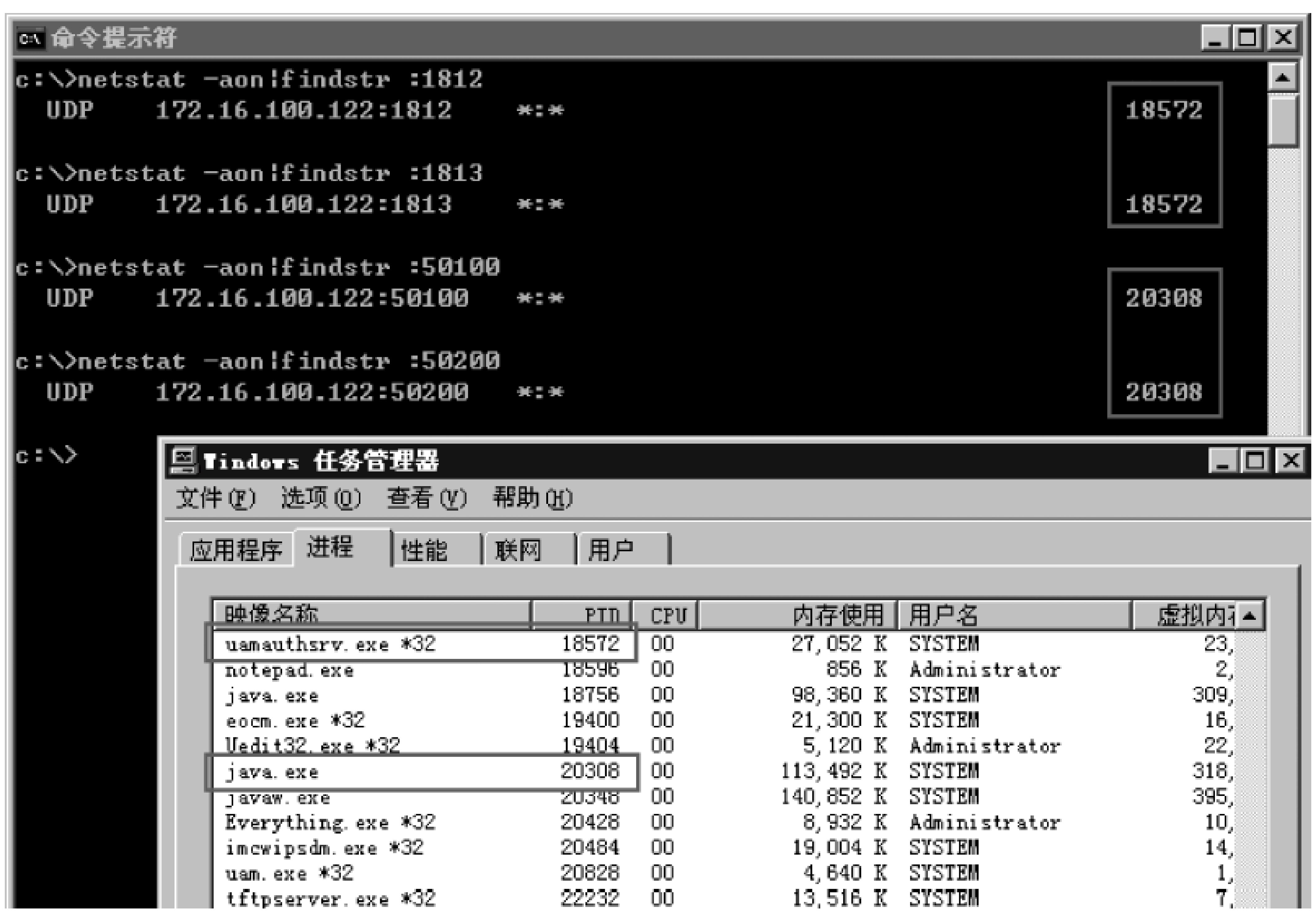


图 8-144　各端口被 uam 相关进程监听情况

说明：

(a) Windows 操作系统中，通过

netstat-aon | findstr：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-145 所示。

```
c:\>netstat -aon|findstr :1812
  UDP    172.16.100.122:1812    *:*          8780
```

图 8-145　命令提示符回显

其中第一列 UDP 所指监听的协议，第二列 10.153.43.100:1812 所指监听的服务器的 IP 和端口号，第三列 *：* 代表此行信息为监听状态，最右一列 8780 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，1812/1813 端口所对应的应为 uam 相关的进程，50100/50200 所对应的为 java 进程。

(3) iMC 服务器和 Portal 设备、终端可达性检查

二维码认证基于 Portal 网页认证，而 Portal 认证是对上行流量的认证，并且需要和 Portal 服务器通信交互 Portal 报文。对于没有禁 ping 的环境，在认证上线之前终端 PC 是可以和 Portal 所在服务器可达的。分别从 iMC 服务器上 ping 接入设备 IP、Portal 设备 IP 和终端 IP。

(4) 普通 Portal 网页认证可用性检查

Portal 认证 Portal 在英语中是入口的意思。Portal 认证可以使用 iNode 客户端或 Web 网页认证，一般将 Portal 认证网站称为门户网站。基本思想：未认证用户上网时，认证设备会强制用户登录到特定 Web 站点，用户可以免费访问该 Web 站点的服务。当用户需要使用互联网中的其他信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。Portal 业务可以为客户提供方便的管理功能，门户网站可以开展广告、社区服务等个性化业务，为了方便客户对门户网站的个性化定制。

Portal 无感知认证必须基于 Web 网页认证，基于 iNode 认证无法实现 Portal 无感知，故在实施 Portal 无感知认证前，必须确保普通 Portal 网页认证正常，再进行 Portal 无感知的配置。有关普通 Portal 认证的排查思路，请参考云图《UAM Portal 认证排错》。

(5) 二维码认证页面配置

二维码认证推送的登录页面和普通 Portal 登录页面有所不同，需要配置专门的二维码认证页面，如果所在的 Portal 端口组中未绑定二维码认证页面，则可以按照如下方法进行配置。

① 单击左侧导航树中的“接入策略管理”→“Portal 服务管理”→“设备配置”命令，进入如图 8-146 所示页面。



图 8-146　“Intelligent Management Center”页面

② 在 Portal 设备列表中,选择 Portal 设备对应的链接,打开“端口组信息配置”对话框,如图 8-147 所示。



图 8-147 选择 Portal 设备对应的链接

③ 在 Portal 端口组列表中单击“增加”按钮,或单击 Portal 端口组对应的链接,打开“增加端口组信息”对话框,如图 8-148 所示。



图 8-148 单击 Portal 端口组对应的链接

④ 配置 Portal 端口组默认认证页面:单击“PC”→“二维码开户与认证”命令,其他参数:与通用的 Portal 认证配置相同。

⑤ iMC EIA 提供了终端页面定制功能,用户也可以根据需要自行基于模板定制二维码认证页面,如图 8-149 所示。

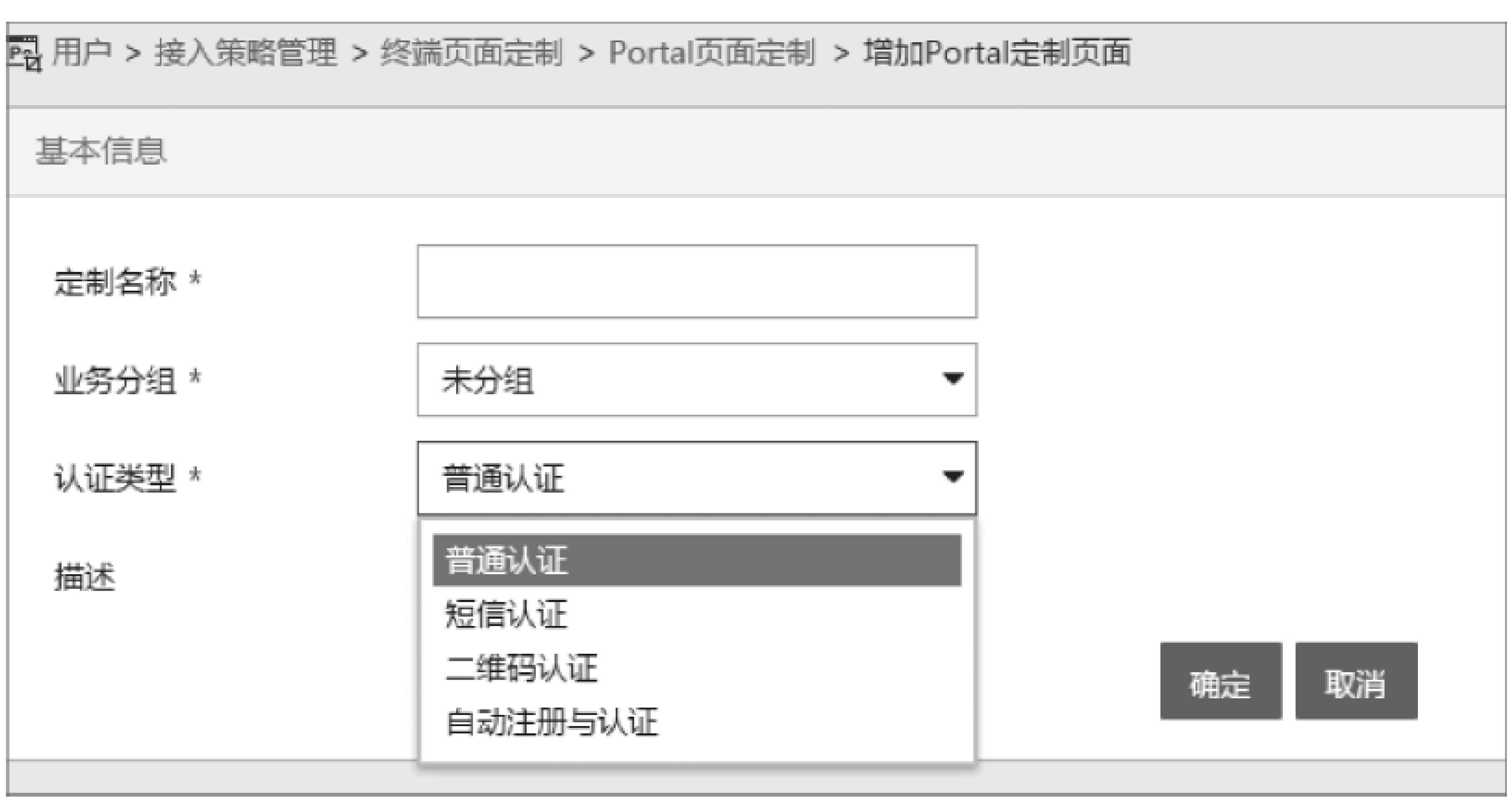


图 8-149 终端页面定制

（6）二维码访客管理员配置检查

访客管理员通过自助页面进行访客审批时，会区分访客管理员的权限，即只有访客预注册时所选的访客管理员或超级访客管理员才能审批。而二维码审批没有权限约束，即所有访客管理员可以扫描任意预注册访客的二维码后进行审批，如果没有配置访客管理员，请参考如下方法配置访客管理员。

① 使用 admin（或其他拥有权限的管理员/维护员）登录 iMC 配置管理台。

② 选择“用户”标签，单击左侧导航树中的“访客管理”→“访客管理员”命令，如图 8-150 所示。



图 8-150 “用户”标签

③ 在访客管理员列表中，单击“增加”按钮，如图 8-151 所示，访客管理员类型选择“访客管理员”，所管理访客的最大有效时长配置为 7 天，审批提醒方式选择“发送审批提醒短信”和“发送审批提醒电子邮件”，如图 8-151 所示。



图 8-151 访客管理员列表

单击“选择接入用户”按钮，弹出如下图所示的窗口。使用查询条件筛选接入用户，选中接入用户后，单击“确定”按钮。

（7）指定一个默认访客管理员

默认访客管理员在自动预注册时使用，不影响二维码审批流程，因此任意指定一个即可。如果系统中已经存在默认访客管理员，则无须再指定。在访客管理员列表中，单击某

个访客管理员对应的默认访客管理员列的“否”链接，即可将该访客管理员指定为默认访客管理员。

(8) 二维码访客服务配置检查

单击“用户”→“访客服务”命令后检查是否配置了访客服务，如果没有访客服务，可以单击“增加”按钮，进入如图 8-152 所示的页面。选择服务后，单击“确定”按钮，即可将所选的服务设置为访客服务。



图 8-152　无访客服务时单击“增加”按钮

在访客服务列表中，单击访客服务对应的“否”链接(见图 8-153)，即可将新增的访客服务设置为自动转正访客服务。



图 8-153　自动转正访客服务

说明：只有不计费和不分配 IP 地址的服务才可以被设置为访客服务。

(9) 二维码访客策略配置检查

访客策略包括“访客参数配置”“访客服务列表”和“访客用户分组列表”3 个配置内容，可以根据客户具体需求配置具体的访客策略参数，如图 8-154 所示。

说明：

① 预注册访客自动转正：如图 8-155 所示，如果选择“允许”表示终端用户预注册为访客后自动转正，而不需要访客管理员审批转正。如果选择“禁止”表示需要访客管理员审批后，预注册访客才能转正。只有当“访客管理”→“访客业务参数配置”中的“访客预注册”设置为“允许”时，该参数才生效。允许访客自动转正时，必须指定默认访客管理员和默认访客服务。在二维码审批方案中，请选择“禁止”，因为审批场景必须由相关的访客管理员进行手工转正。

② 访客密码通知方式：选择告知访客登录密码等信息的方式。告知方式包括短信和电子邮件，可以同时选择两种方式。如果告知方式为短信，则需要启用短信功能，详细说明请参



图 8-154　配置访客策略参数



图 8-155　预注册访客自动转正

见短信功能配置；短信的内容在“消息下发”中定制。如果告知方式为电子邮件，邮件的内容由 UAM 预置，无法修改；同时只有在 iMC PLAT 中配置正确的邮件服务器，才能成功发送邮件。如果未选择任何一种方式，表示不将密码通知到访客。

③ 访客预注册后显示二维码：访客预注册以及预注册自动转正(除 BYOD 方式)的结果页面是否显二维码。

④ 访客生效方式：如果选择“手工指定生效时间”表示访客管理员可以手工指定所管理访客的生效时间和失效时间，如果选择“首次上线生效”表示访客首次上线后更新生效时间和失效时间。除了移动访客管理自助平台注册的访客，其他方式注册的访客转正时，访客生效时间都受该参数控制。

⑤ Portal 无感知认证最大绑定数：如果设置为 0～255 表示使用该账号进行 Portal 无感知认证的终端数不能超过所设置的值。0 表示不支持绑定。只有当“访客管理”→“访客业务参数配置”中的“访客预注册”设置为“允许”时，该参数才生效。

⑥ 默认访客有效时长：输入默认情况下，访客的有效时长。注册访客时，如果未设置或

无法设置失效时间，则访客的失效时间取该参数和"所管理访客的最大有效时长"的较小值。"所管理访客的最大有效时长"在增加访客管理员时配置，具体请参见增加访客管理员。

⑦ 访客密码有效时长：输入访客密码的有效时长，从访客生效时开始计算。访客只在密码失效前才能接入网络。如果该参数保持为空，则表示访客密码永不失效。

⑧ 访客密码生成规则：系统自动生成访客密码的规则。UAM 支持 3 种规则，即 n 位数字、n 位字母和 n 位数字＋字母的组合。该规则对访客注册过程中手工输入的密码无效。

⑨ 访客在线数量限制默认值：输入访客注册页面中"在线数量限制"默认显示的值。

⑩ 访客在线数量限制最大值：输入访客注册页面中"在线数量限制"可以配置的最值。

(10) 二维码认证使用方法合理性检查

iMC 访客二维码认证主要有以下两种应用方式。

① 审批二维码：访客访问任意站点被重定向到二维码注册和认证页面，并自动进行预注册和生成审批二维码。访客管理员直接扫描二维码进入审批页面并对访客进行审批，审批完成后，访客即可自动接入网络。

② 认证二维码：访客管理员在移动访客管理自助平台中创建访客，并生成认证二维码。访客直接扫描二维码即可完成认证。

在这两种方式下，iMC 中访客相关的配置基本相同，差别在于实际的使用流程不同。

在完成二维码认证环境的实施后，如何使用二维码认证格外重要，如果您对二维码的使用流程存在疑问，请参考如下操作流程。

① 审批二维码方案使用流程

第 1 步，访客连接 Wi-Fi。

访客使用智能终端 A(访客自带的智能终端)连接 SSID。打开浏览器，访问任意地址。浏览器自动跳转到二维码开户和认证页面，并自动完成访客预注册且在页面上显示审批二维码，如图 8-156 所示。



图 8-156　显示审批二维码

第 2 步，访客管理员审批。

访客管理员使用智能终端 B(访客管理员的智能终端)扫描智能终端 A 上的二维码，智能终端 B 直接进入移动访客管理自助平台进行审批，如图 8-157 所示。

在访客审批页面，直接单击"转正"，即可将预注册访客转正。

第 3 步，访客上线时间。

如果访客在智能终端 A 上生成审批二维码未超过 1 分钟，则访客管理员在智能终端 B 上审批完成后的 5 秒钟内，智能终端 A 自动进行 Portal 认证并上线，结果如图 8-158 所示。

如果生成审批二维码已经超过 1 分钟，智能终端 A 上会显示如图 8-159 所示的失败信息。



图 8-157　访客管理员审批

请单击“重试”链接即可完成上线。

② 认证二维码方案使用流程

第 1 步，访客管理员注册访客。

访客管理员在智能终端 B(访客管理员的智能终端)上使用浏览器输入 http://ip: port/selfservice/mlogin.jsf(移动访客管理自助平台的 URL)，打开登录页面，如图 8-160 所示。



图 8-158　访客上线时间



图 8-159　审批二维码已经超过 1 分钟



图 8-160　访客管理员注册访客

输入访客管理员账号/密码后进入管理平台。单击页面下方的“访客注册”按钮，然后单击在页面右上角的“快捷注册”按钮，弹出确认提示，如图 8-161 所示。



图 8-161 “快捷注册”对话框

单击“是”按钮完成访客注册，并进入结果页面。结果页面中显示了认证二维码，如图 8-162 所示。

第 2 步，访客扫描上线。

访客使用智能终端 A（访客自带的智能终端）连接网络。扫描上图的二维码完成认证并上网。扫描完成后，直接跳转到认证成功页面，如图 8-163 所示。



图 8-162 结果页面

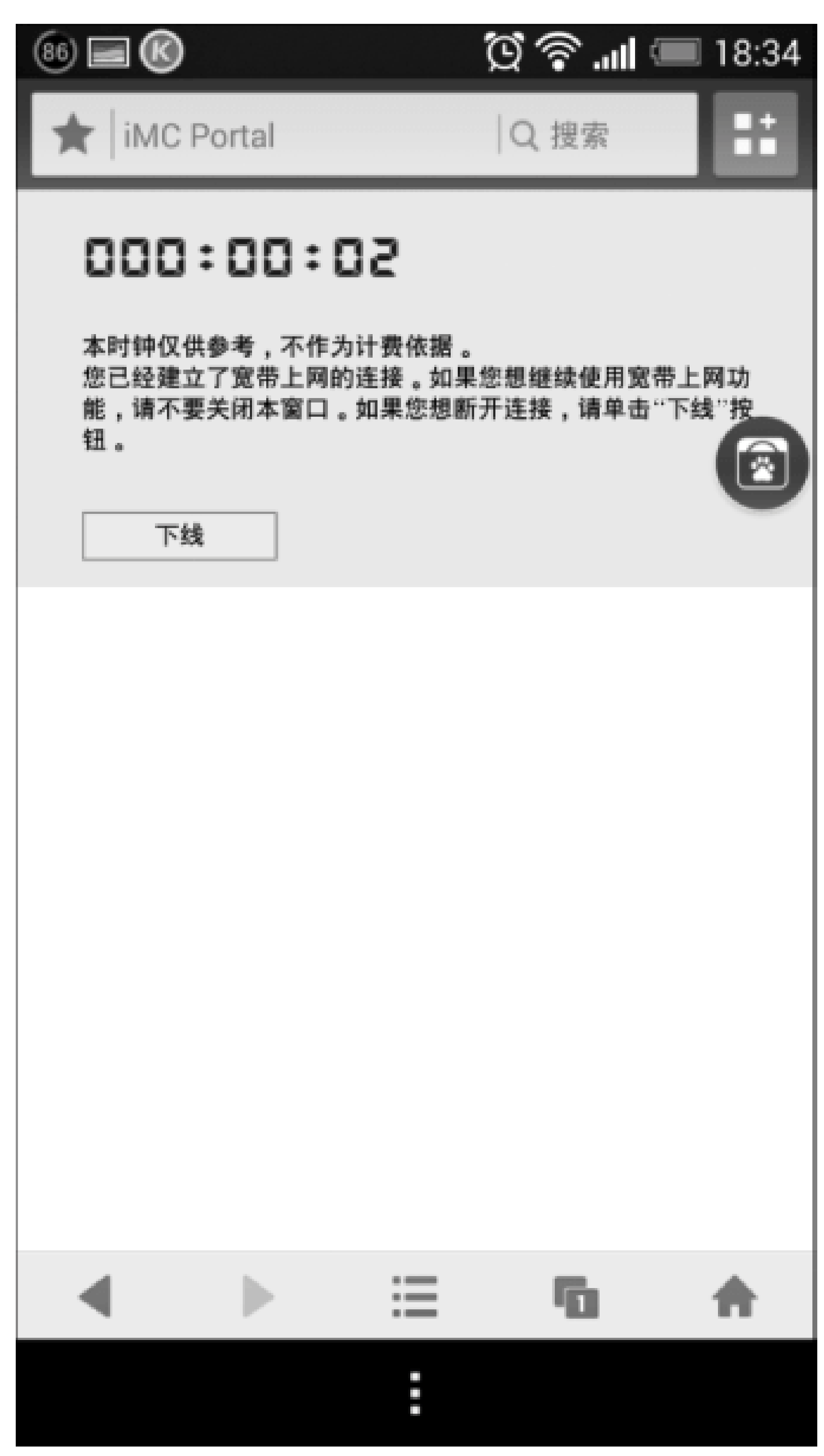
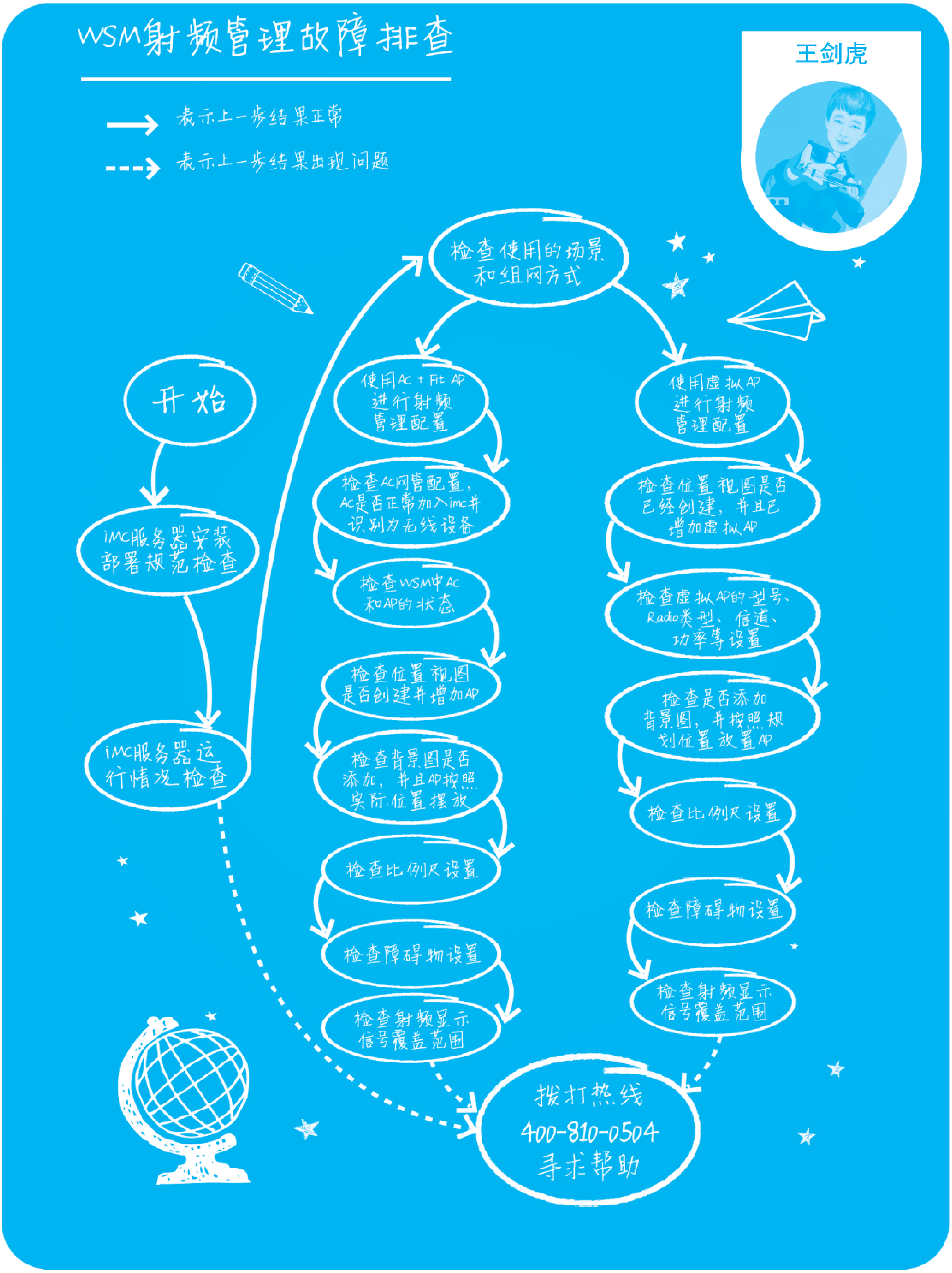


图 8-163 访客扫描上线



WSM射频管理故障排查
表示上一步结果正常
表示上一步结果出现问题
王剑虎
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
检查使用的场景和组网方式
使用AC + Fit AP进行射频管理配置
检查AC网管配置，AC是否正常加入imc并识别为无线设备
检查WSM中AC和AP的状态
检查位置视图是否创建并增加AP
检查背景图是否添加，并且AP按照实际位置摆放
检查比例尺设置
检查障碍物设置
检查射频显示信号覆盖范围
使用虚拟AP进行射频管理配置
检查位置视图是否已经创建，并且已增加虚拟AP
检查虚拟AP的型号、Radio类型、信道、功率等设置
检查是否添加背景图，并按照规划位置放置AP
检查比例尺设置
检查障碍物设置
检查射频显示信号覆盖范围
拨打热线
400-810-0504
寻求帮助

08 iMC 管理软件 〉 8.1 业务软件：iMC 〉 8.1.19 WSM 射频管理故障排查 〉 步骤详解

1. 开始

WLAN(Wireless Local Area Network,无线局域网)是计算机网络与无线通信技术相结合的产物。由于 WLAN 在部署时不需要考虑复杂的布线、优化和变迁,因此 WLAN 系统便于搭建和使用,具有安装便捷、高移动性和易扩展等特点,所以其应用越来越广泛。

WSM 射频管理根据 AP 的 Radio 类型、发射功率,以及周围环境(混凝土墙、玻璃窗、门等)对无线信号衰减的影响,计算和绘制 AP 的 RF 覆盖效果图,支持按信号强度、接入速率、信道 3 种方式进行展示。用户可以在位置视图拓扑中根据实际环境增加障碍物,并指定障碍物的类型和厚度。

实现了射频管理功能后,用户可以方便地看到无线网络中的信号覆盖情况和信道冲突情况,进而通过调节 Radio 的发射功率和信道等参数,使无线网络中的信号覆盖达到最佳效果。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》,检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求,请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格,当网络中管理的 AP 数量较多,需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将 WSM 组件分布式部署在了性能良好的服务器上,重点需要检查内存占用是否过高,内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求,操作系统和数据库是否为 64 位,建议使用 64 位系统。

② 单击"开始"→"智能部署监控代理"命令,选择"部署"标签,检查"无线业务管理"功能模块是否已经部署,如图 8-164 所示。



图 8-164 "无线业务管理"功能模块部署情况

(2) iMC 服务器运行情况检查

打开部署监控代理,查看 jserver、imcwlandm 进程是否正常启动,如图 8-165 所示。

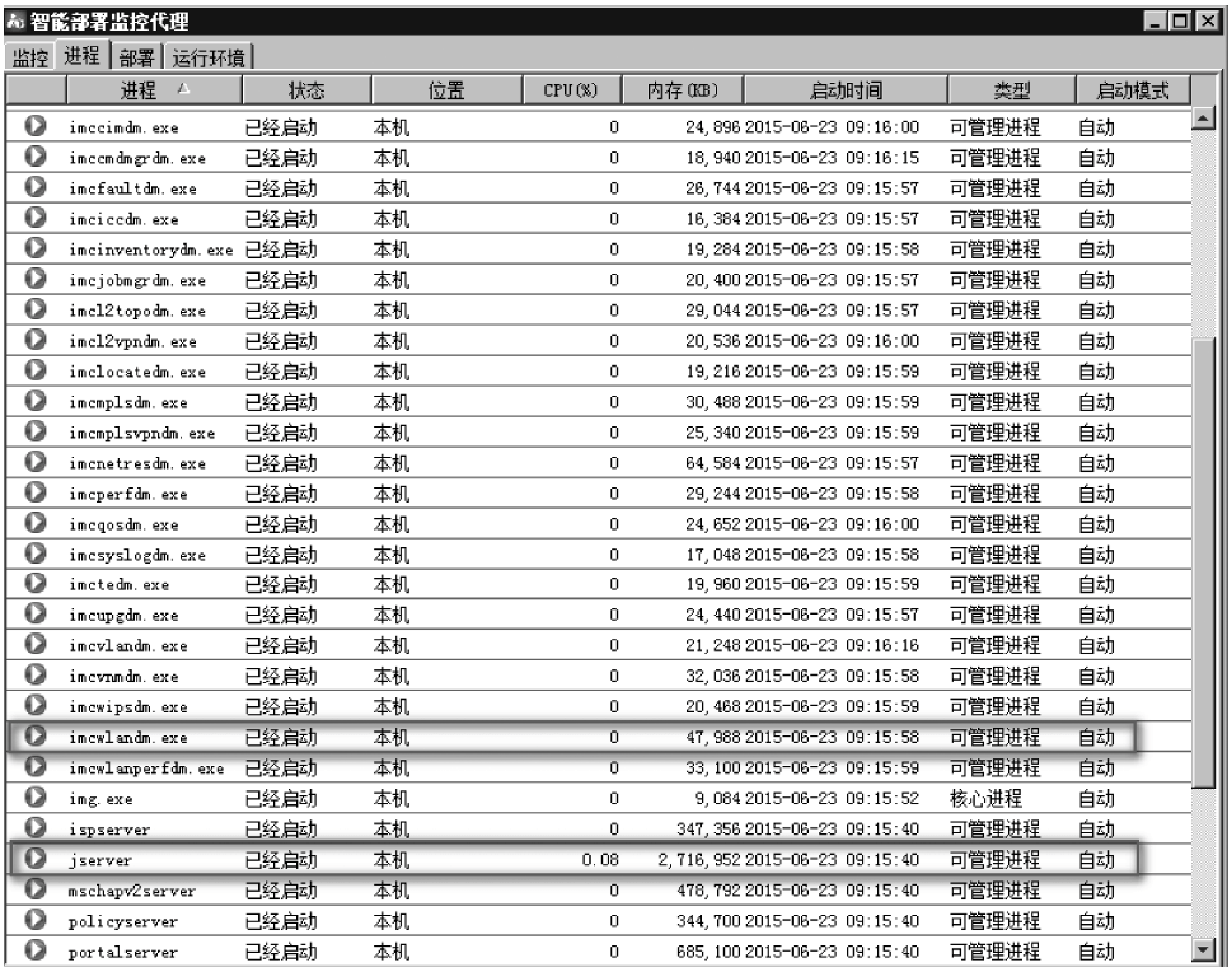


图 8-165　各进程启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为"自动启动"。

如果无线进程 imcwlandm 启动失败，需要找到 iMC\server\conf\log\imcwlandm.log 日志，查看最后一行，一般可能有如下几种情况。

① 如果日志中出现 Initialize process enviorment failed.就是说明有其他进程占用了进程端口。检查服务器 8080、9091、161、162、61616、61626 等端口是否被 iMC 相关进程所监听，如图 8-166 所示。



图 8-166　各端口被 iMC 相关进程监听情况

说明：

(a) Windows 操作系统中，通过

netstat -aon | *findstr* ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-167 所示。

```
C:\Users\Administrator>netstat -ano | findstr 9091
  TCP    0.0.0.0:9091           0.0.0.0:0              LISTENING       21508
  TCP    [::]:9091              [::]:0                 LISTENING       21508
```

图 8-167　命令提示符回显

其中第一列 TCP 所指监听的协议，第二列 0.0.0.0:9091 所指监听的服务器的 IP 和端口号，第三列 LISTENING 代表此行信息为监听状态，最右一列 21580 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，9091 端口所对应的应为 JServer 相关的进程，61616/61626 所对应的为部署监控代理相关进程。

② 如果日志中出现 CWlanDBOper::getWlanDataDB error, db opt error!!，这个错误表示启动查表时失败，看这条语句的前三行，分析 SQL 语句是哪种错误。分析不明白的需要拨打 400 电话寻求技术支持。

③ 有一种情况只针对 Linux 的环境，如果出现 imcwlandm 进程启动失败，并且没有无线后台日志。这时候需要在 shell 中执行启动脚本，看一下具体失败原因。在 WSM 7.0 E0202P03 及之后版本，在 iMC/server/bin 文件夹下都有一个 start_wlan.sh 文件。没有的话，可以通过使用这里提供的 start_wlan.sh 文件，在当前目录中执行./start_wlan.sh 命令。

示例：使用 start_wlan.sh 脚本启动时，显示 load libfreebl3.so 错误，缺少这个文件。解决办法就是从正常的 Linux 机器中，/usr/lib/目录下拷贝 libfreebl3.so 文件到该局点 Linux 相同目录下。

(3) 确认使用哪种场景和相关组网方式

① 使用 AC + Fit AP 进行射频管理配置，请转至(4)继续排查。

应用场景：用户已经搭建了无线网络，部署好 AP，希望从 iMC 网管中看到无线网络中的实际信号覆盖情况。比如：某学校的教学楼一楼已经部署了无线网络。

组网环境需求如下。

(a) 管理主机、服务器集群、AC(WX5004)路由可通。

(b) AP 在 AC 上上线，状态正常。

(c) 服务器集群运行 iMC，并有 WSM 组件射频管理典型配置组网图(AC+Fit AP)，如图 8-168 所示。

② 使用虚拟 AP 进行射频管理配置，请转至(5)继续排查。

应用场景：用户已经搭建了无线网络，需要进行扩容的情况。比如：某学校的教学楼一楼和二楼已经部署了无线网络，打算在三楼也部署无线网络。由于三楼和其他楼层的建筑格局不一样，用户希望在实际购买前，能够进行网络规划，得到需要 AP 的型号和数量信息以及恰当的摆放位置，需要使用 WSM 网规功能(虚拟 AP 射频管理)来满足相关需求。

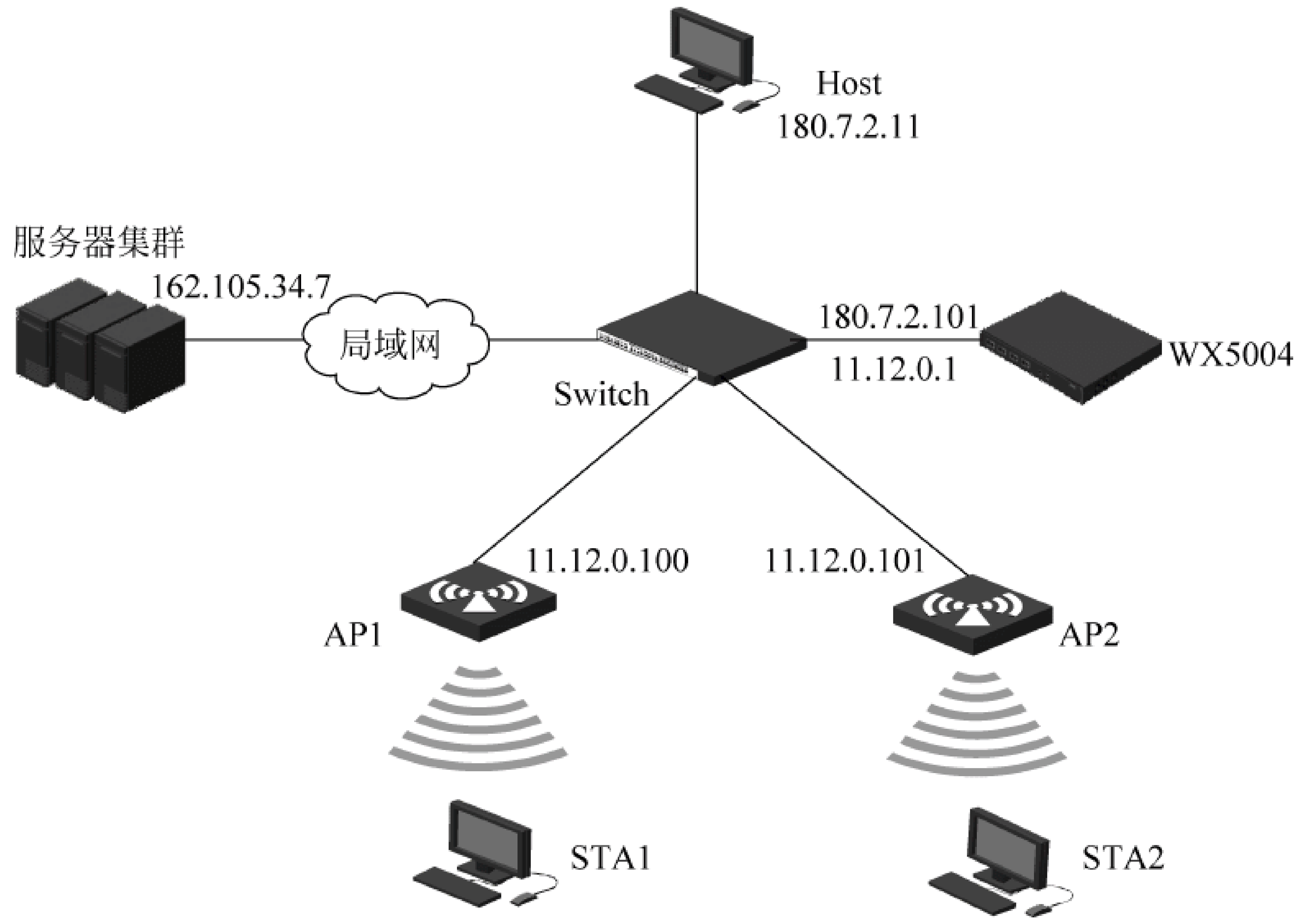


图 8-168　WSM 组件射频管理典型配置组网图

组网环境需求：安装、启动 iMC WSM。

(4) 使用 AC ＋ Fit AP 进行射频管理配置的排查步骤

按照如下的思路检查 iMC WSM 射频管理的配置。

① 检查 AC 网管配置。

② 检查 AC 是否加入 iMC，WSM 是否正常识别 AC 和 AP。

③ 按如下步骤检查 iMC WSM 射频管理配置是否正确。

(a) 检查是否已经创建位置视图并根据实际情况添加 AP。

(b) 打开位置拓扑，检查是否已经添加背景图，并且按照实际位置在图上放置 AP。

(c) 是否为背景图设置合适的比例尺。

(d) 是否在背景图上据实添加障碍物。

(e) 是否可以正常显示信号覆盖范围。

具体检查配置的步骤如下。

① 检查 iMC 是否已经增加设备 AC，AC 是否识别为无线设备。

在 iMC“资源”标签，单击资源管理导航树中的“增加设备”命令，进入增加设备页面，正确填写相关参数，增加设备，如图 8-169 所示。

确认 AC 的设备类型已经被识别为无线设备，如图 8-170 所示。

② 检查 WSM 中 AC 是否增加成功，AP 是否自动增加成功。

在 WSM 的资源管理，无线控制器列表中，查看 AC、AP 是否自动增加成功，如图 8-171 所示。

如果 AC 设备未正常识别或未在 WSM 中添加成功，请参考云图《WSM 无法识别或同步 AC 故障排查》排查。

③ 检查 WSM 中射频管理是否按照如下步骤进行配置。

选择“业务”标签，单击无线业务管理导航树中的“视图管理”菜单组中的“位置视图”命令，



图 8-169 增加设备页面



图 8-170 确认 AC 的设备类型已经被识别为无线设备



图 8-171 无线控制器列表

进入位置视图管理页面，如图 8-172 所示。



图 8-172　位置视图管理页面

单击“增加”按钮，进入增加位置视图页面，如图 8-173 所示。



图 8-173　增加位置视图页面

输入位置名，如“21 楼 7 层”，选择位置类型；选择是否热点；如果选择是热点，设置热点扩展属性。

说明：

(a) 位置类型包括以下 4 种类型：区域、楼宇、楼层和房间，增加位置视图时默认为“区域”类型。“区域”类型的位置视图可以增加任意类型的子位置视图；“楼宇”类型的位置视图只能增加“楼层”和“房间”类型的子位置视图；“楼层”类型的位置视图只能增加“房间”类型的子位置视图；“房间”类型的位置视图不能增加子位置视图。

(b) 设置为热点的位置视图不能增加子位置视图。

单击“确定”按钮，完成增加位置视图，如图 8-174 所示。

单击“21 楼 7 层”链接，进入“子位置”→“设备列表”页面，如图 8-175 所示。

单击“增加到本位置”按钮，打开“选择设备”窗口。可以根据条件查询 AP。

说明：视图中已经存在的设备，不会再出现在选择设备窗口的设备列表中，以避免重复加入设备，如图 8-176 所示。



图 8-174 完成增加位置视图



图 8-175 设备列表页面



图 8-176 选择设备窗口

选中位置视图中的AP前的复选框，单击“确定”按钮。完成向位置视图中增加设备，如图8-177所示。



图8-177 在位置视图中增加设备

单击“查看拓扑”链接，打开位置视图拓扑，如图8-178所示。



图8-178 “查看拓扑”链接

打开位置视图拓扑，如图8-179所示。

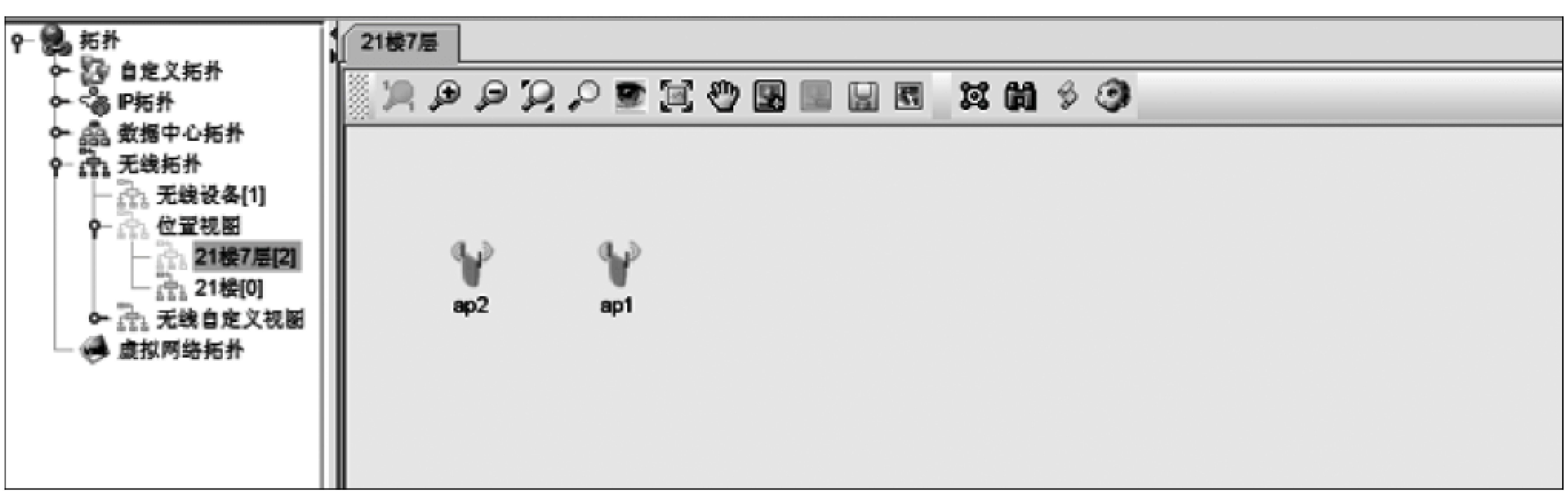


图8-179 位置视图拓扑

在位置视图拓扑工具栏中单击“添加背景图”按钮，选择背景图片，并单击“设置”按钮。

说明：设置拓扑背景图有两种方式：“用户上传背景图片”和“从背景图库中选择”，“用户上传背景图片”使用过的背景图片自动加入图库，支持的图片格式、大小、尺寸等要求见页面提示。

单击“添加背景图”按钮，如图8-180所示。

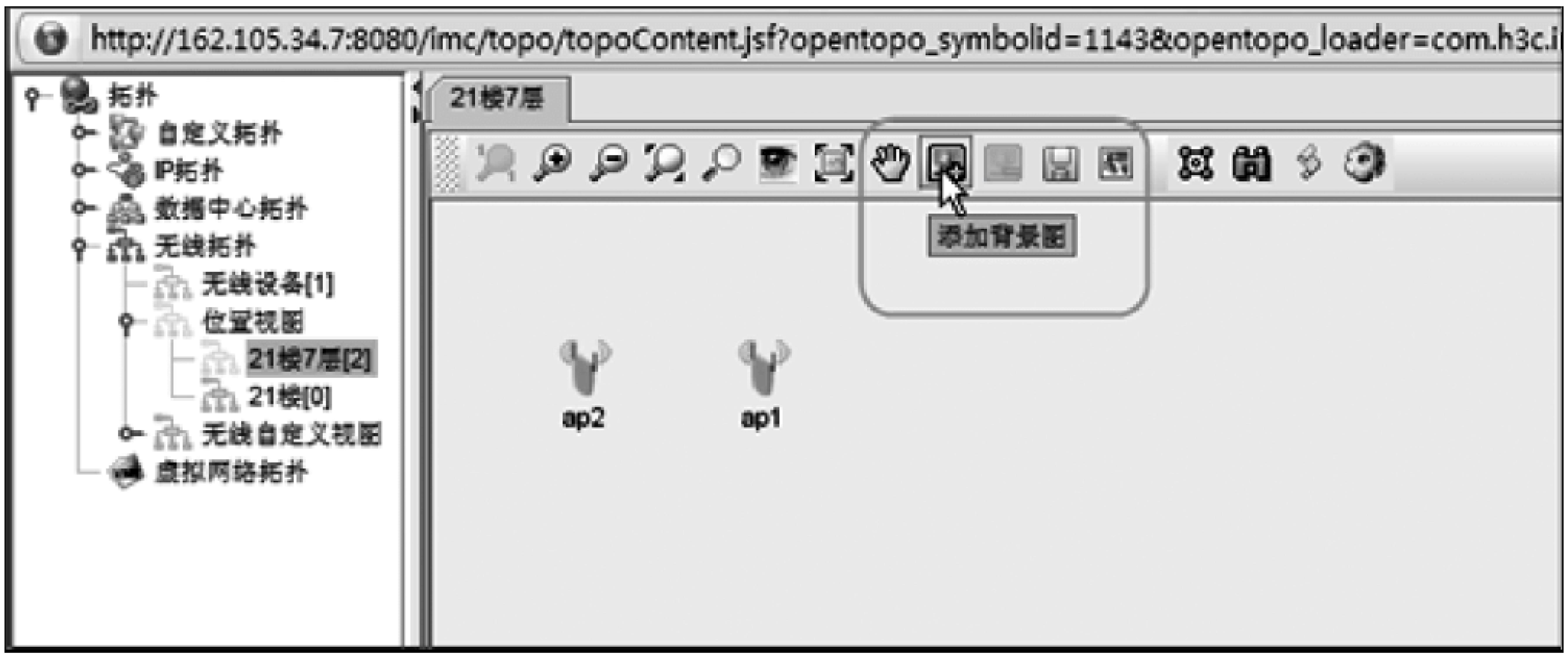


图 8-180　单击"添加背景图"按钮

设置拓扑背景图,如图 8-181 所示。



图 8-181　设置拓扑背景图

设置背景图片成功,如图 8-182 所示。

单击右键菜单中的"设置比例尺"命令,按住鼠标左键,在背景图的两点之间画一条线,放开鼠标左键,在弹出的"指定实际长度"对话框中指定这两点间的实际长度,单位为米。

单击"设置比例尺"命令,如图 8-183 所示。

"指定实际长度"对话框,如图 8-184 所示。

将 AP 拖动到背景图中实际所在的位置,单击工具栏中的"保存"按钮,如图 8-185 所示。

增加障碍物：如果实际位置视图环境中存在障碍物,单击工具栏中的"增加障碍物"按钮增加障碍物,如图 8-186 所示。

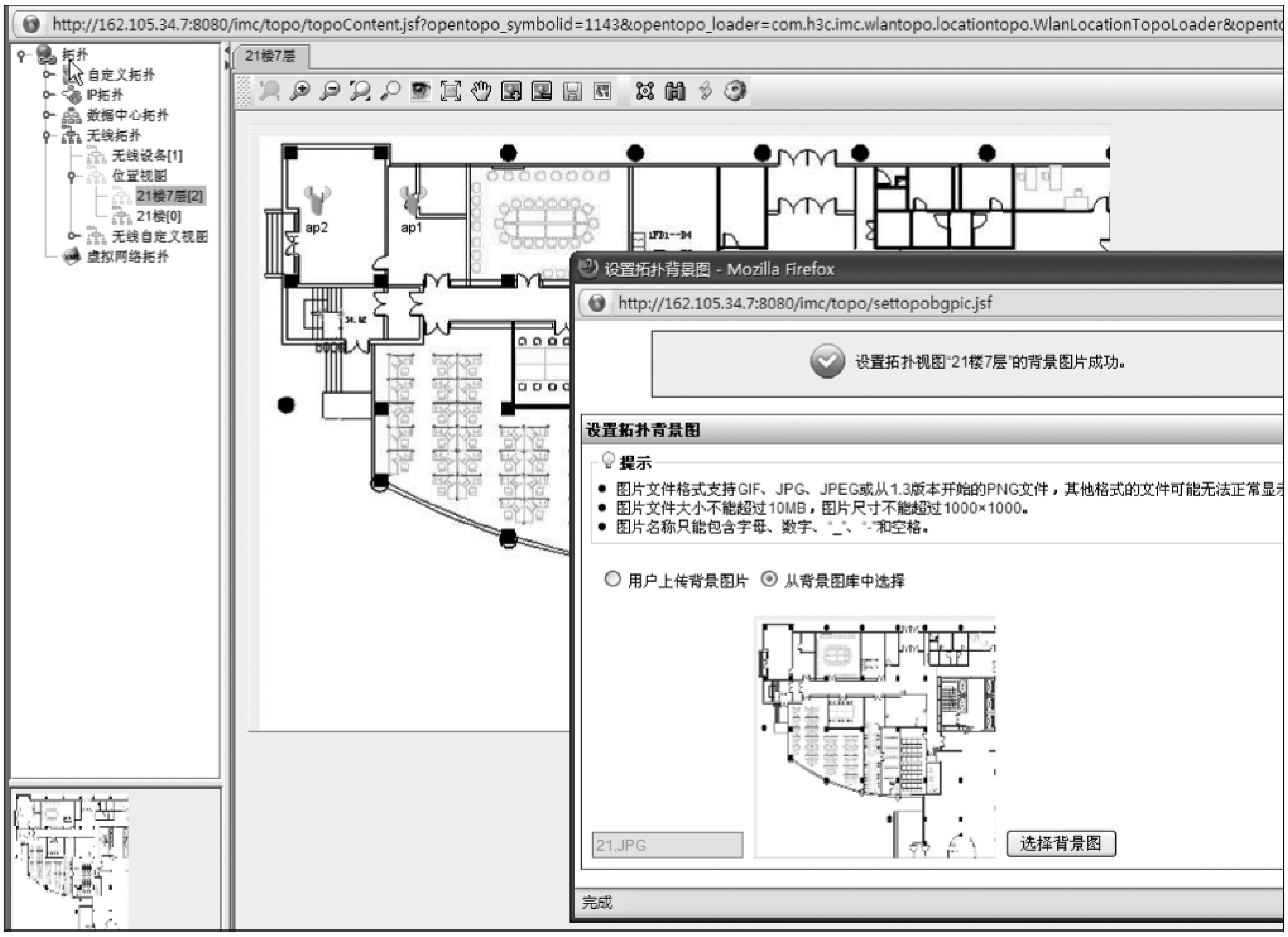


图 8-182 设置背景图片成功

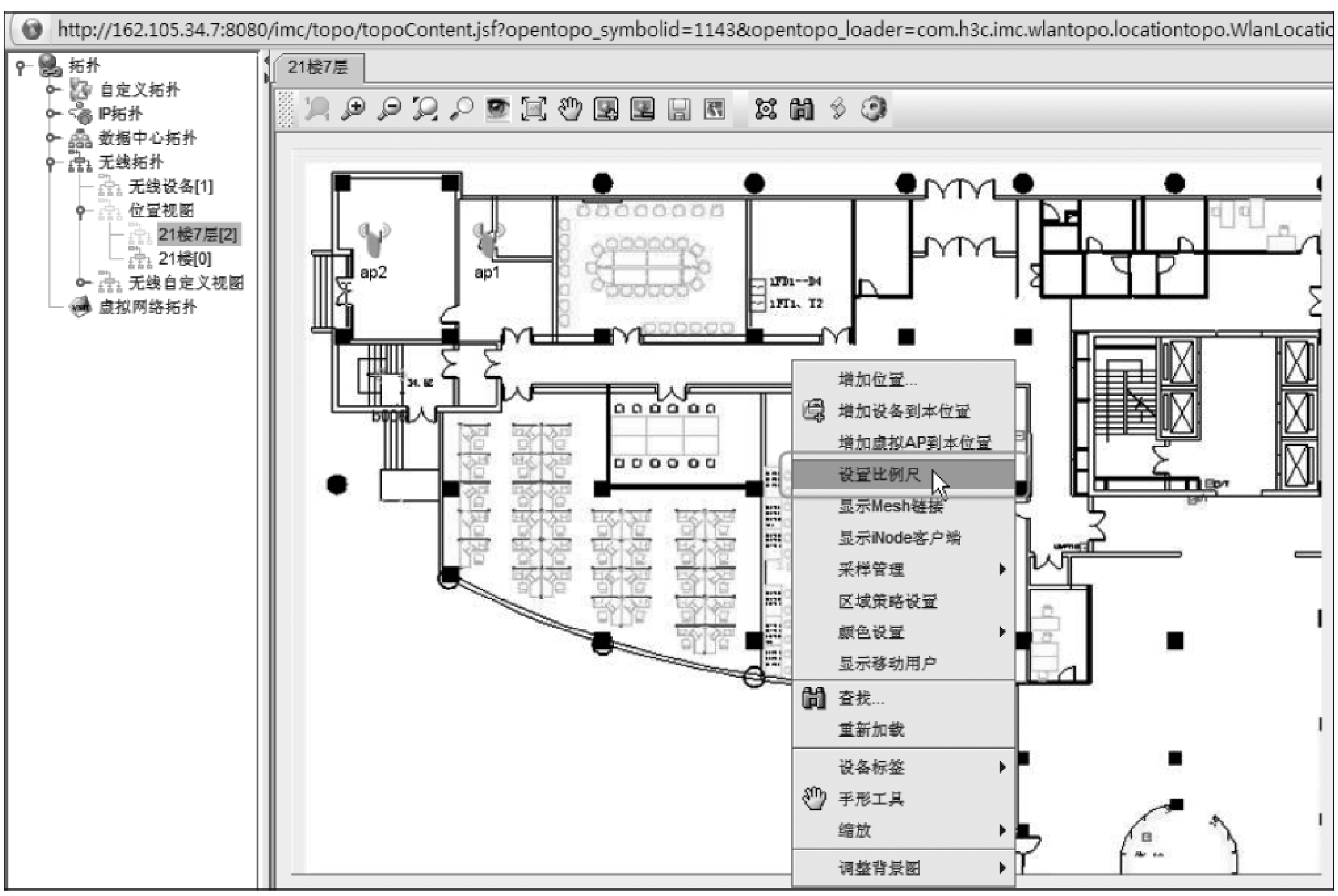


图 8-183 单击“设置比例尺”命令



图 8-184 “指定实际长度”对话框

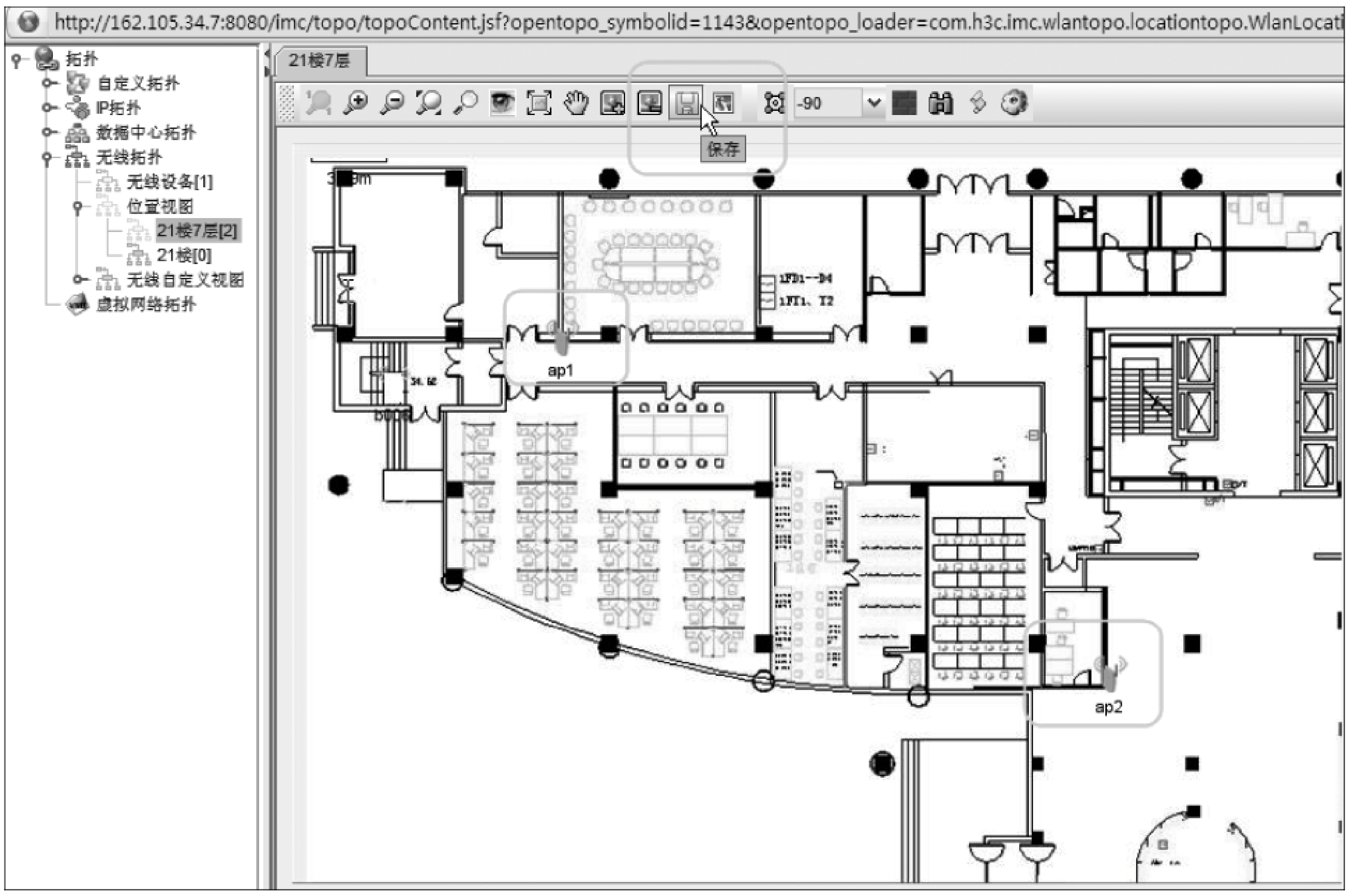


图 8-185 将 AP 拖动到背景图中

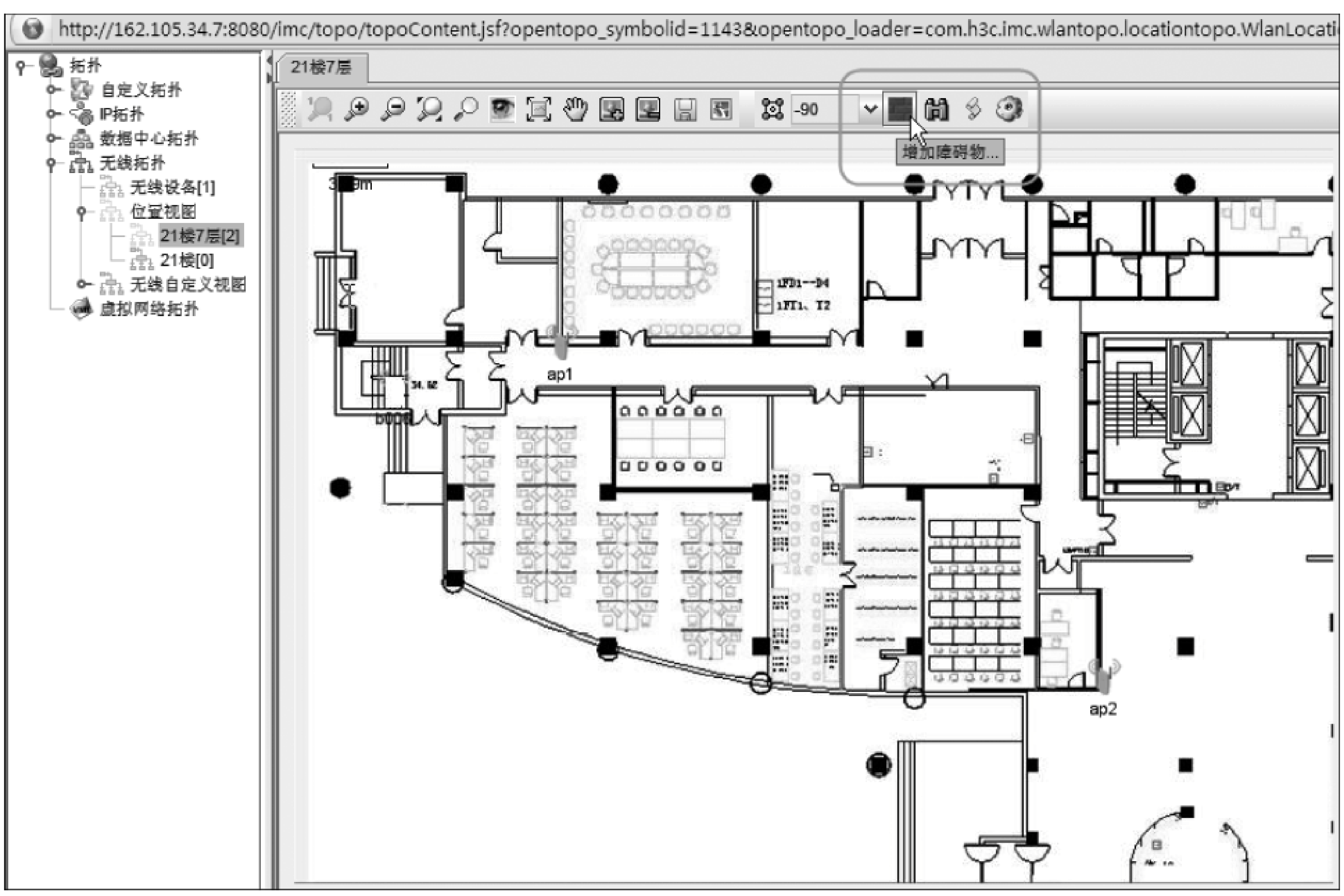


图 8-186 增加障碍物

在“增加障碍物”对话框中选择合适的形状、类型，指定厚度，单击“确定”按钮开始增加，如图 8-187 所示。



图 8-187 “增加障碍物”对话框

设置障碍物后，根据实际增加障碍物，增加完成后，单击“指针工具”按钮结束增加，如图 8-188 所示。

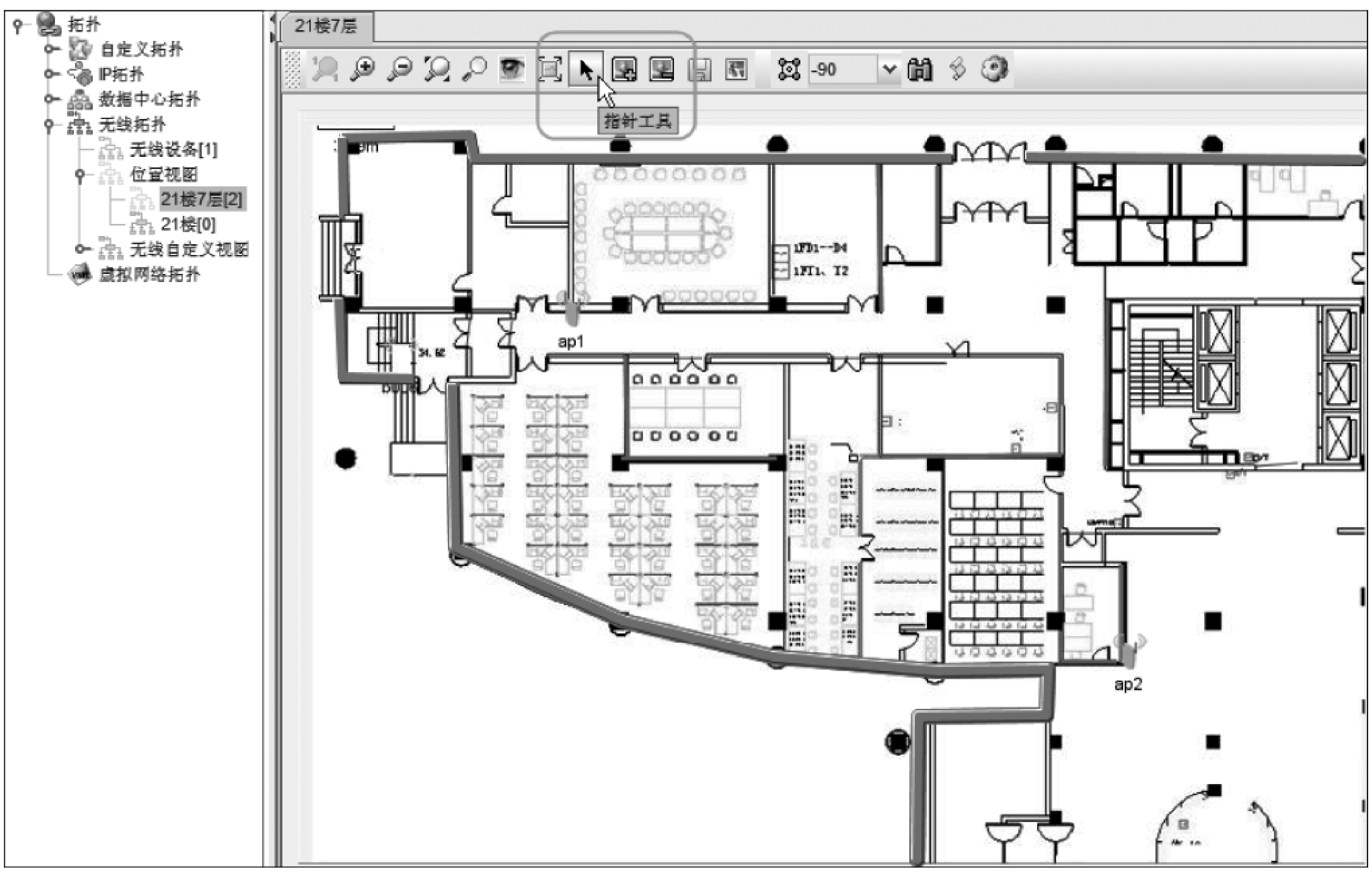


图 8-188 结束增加

④ 检验配置结果：查看信号覆盖范围。

在位置视图拓扑中，单击右键菜单中的“显示信号覆盖范围”命令，如图 8-189 所示。

按信号强度显示信号覆盖范围，单击鼠标左键可以显示该处的信号强度。单击工具栏中的“接收灵敏度”按钮可以修改查看的最低信号强度。

按信号强度显示信号覆盖范围，如图 8-190 所示。

各级信号强度对应的颜色用户可以进行自定义，设置信号强度颜色，如图 8-191 所示。

按速率显示信号覆盖范围，单击鼠标左键可以显示该处的速率，如图 8-192 所示。

各级速率对应的颜色用户可以进行自定义，设置速率颜色，如图 8-193 所示。



图 8-189 “显示信号覆盖范围”菜单

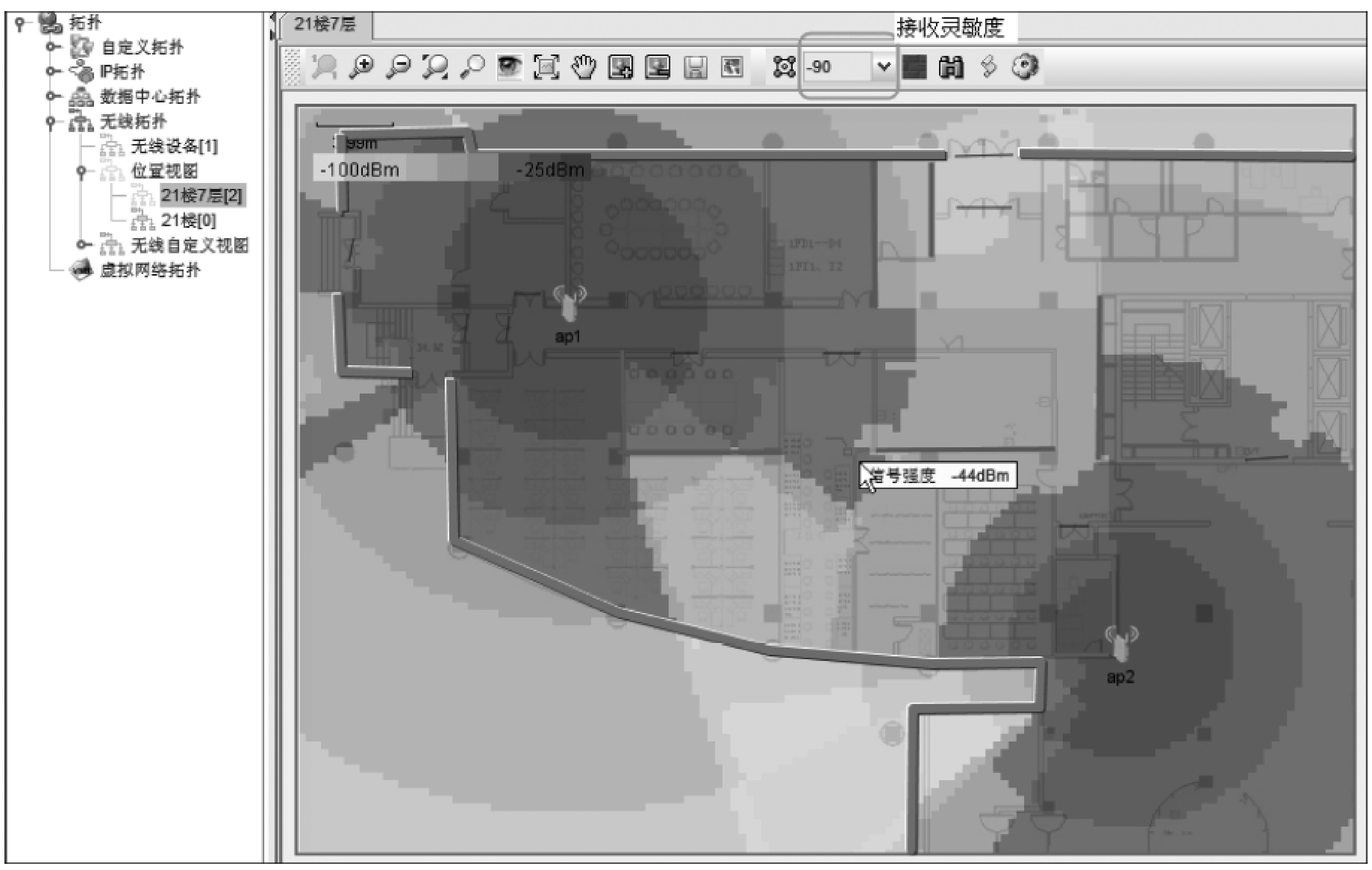


图 8-190 按信号强度显示信号覆盖范围

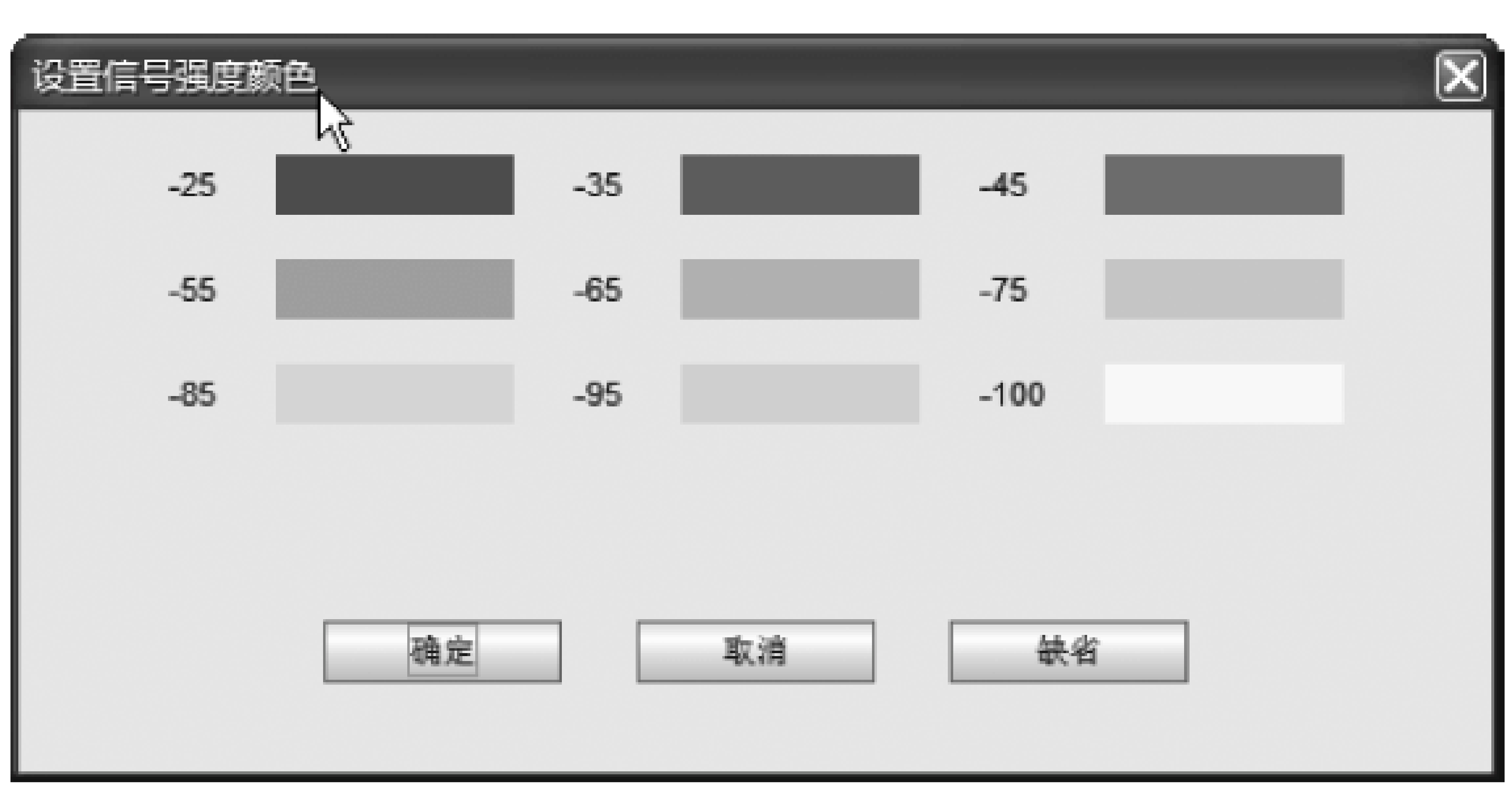


图 8-191 “设置信号强度颜色”对话框

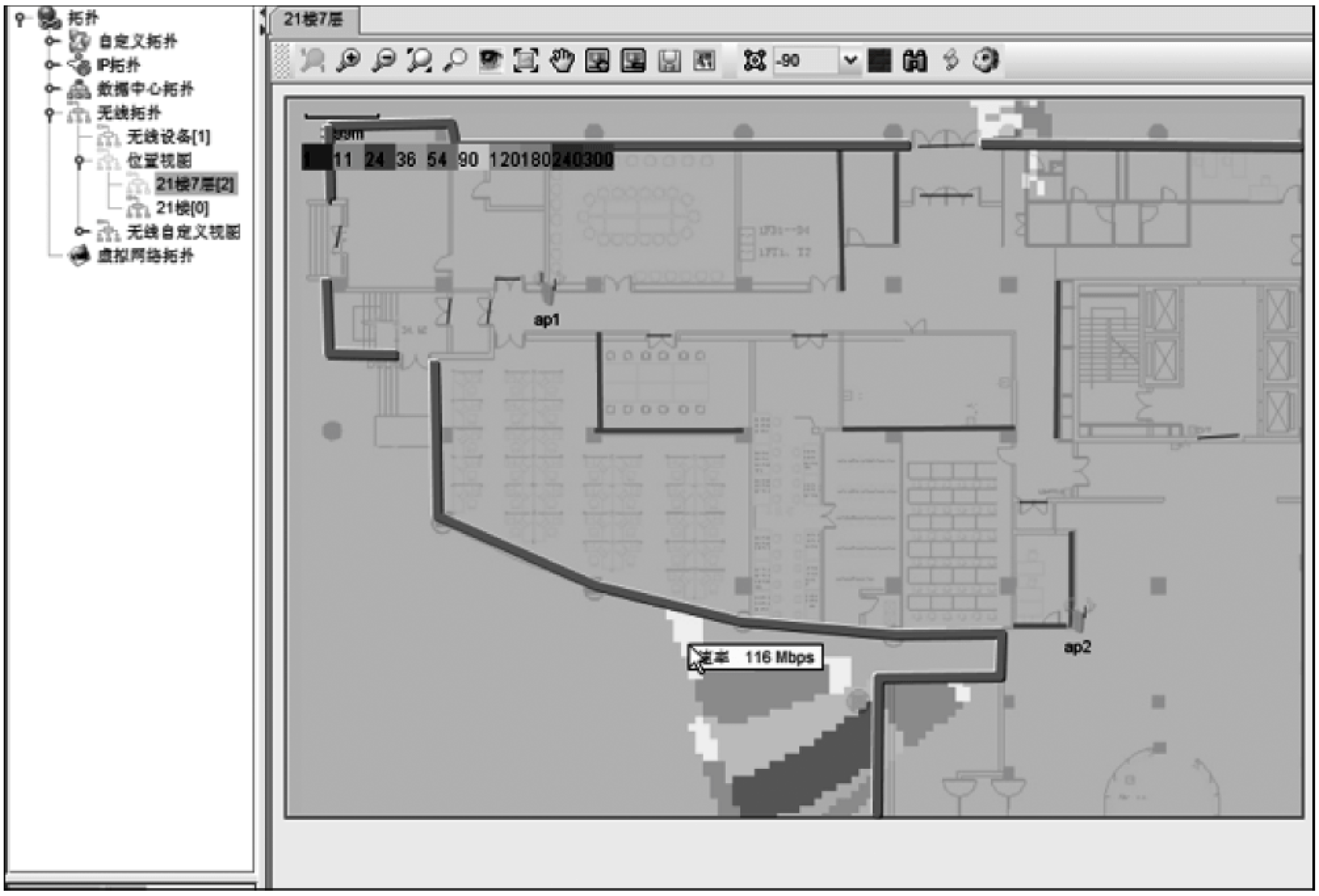


图 8-192　显示速率

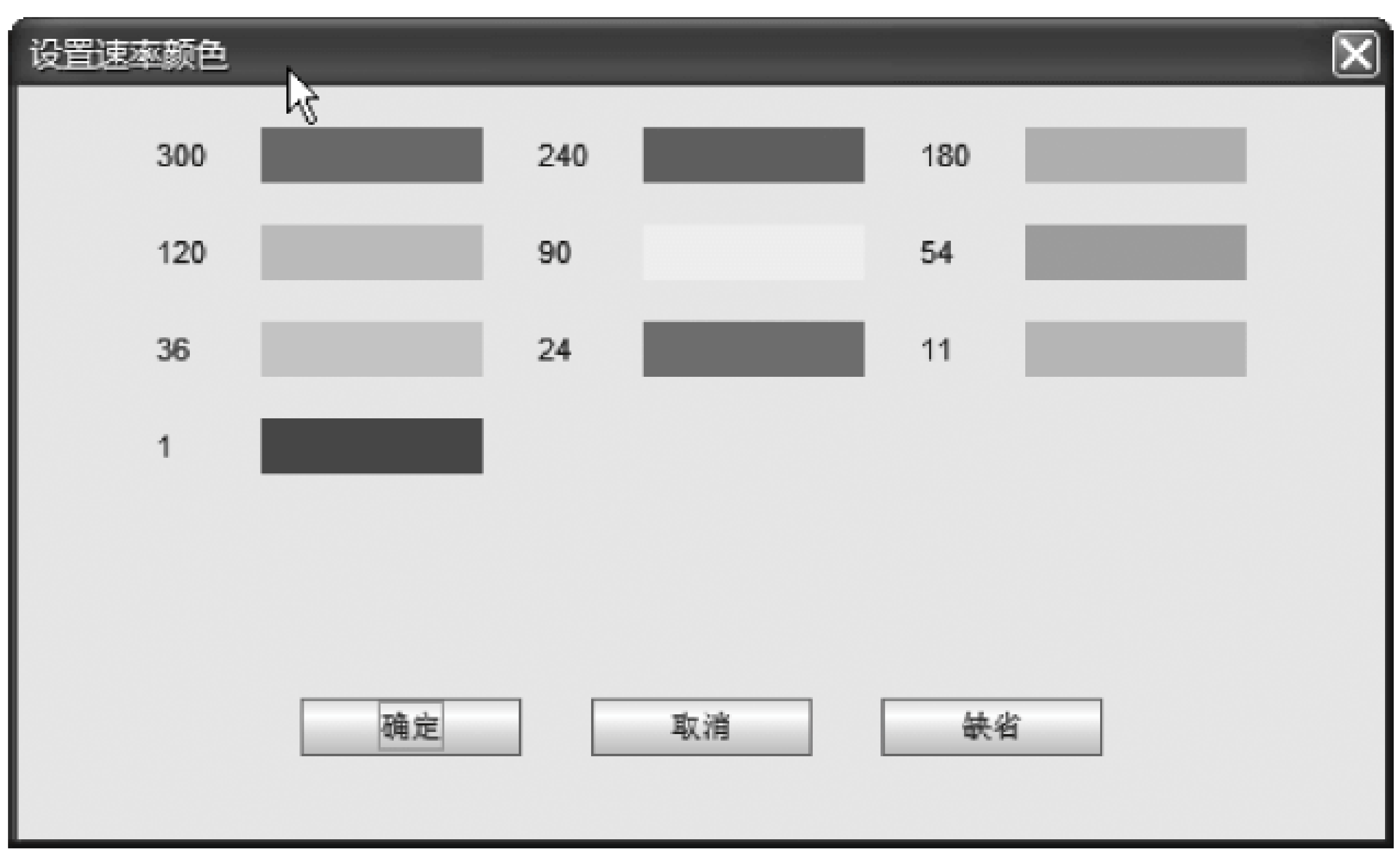


图 8-193　“设置速率颜色”对话框

按信道显示信号覆盖范围，单击鼠标左键可以显示该处的信道冲突情况。对于有信道冲突的区域，可调整 AP Radio 的功率和信道等配置后再次查看信号覆盖范围。对于有信道重叠的区域，颜色也有响应的叠加颜色效果，如图 8-194 所示。

各信道对应的颜色用户可以进行自定义，设置信道颜色，如图 8-195 所示。

(5) 使用虚拟 AP 进行射频管理配置的排查步骤

按照如下的思路检查使用虚拟 AP 配置 iMC WSM 射频管理(WSM 网规功能)。

① 检查是否已经创建位置视图，并且增加虚拟 AP。

② 打开位置拓扑，检查是否添加背景图，并且按照规划位置在图上放置 AP。

③ 是否为背景图设置合适的比例尺。

④ 是否在背景图上据实添加障碍物。

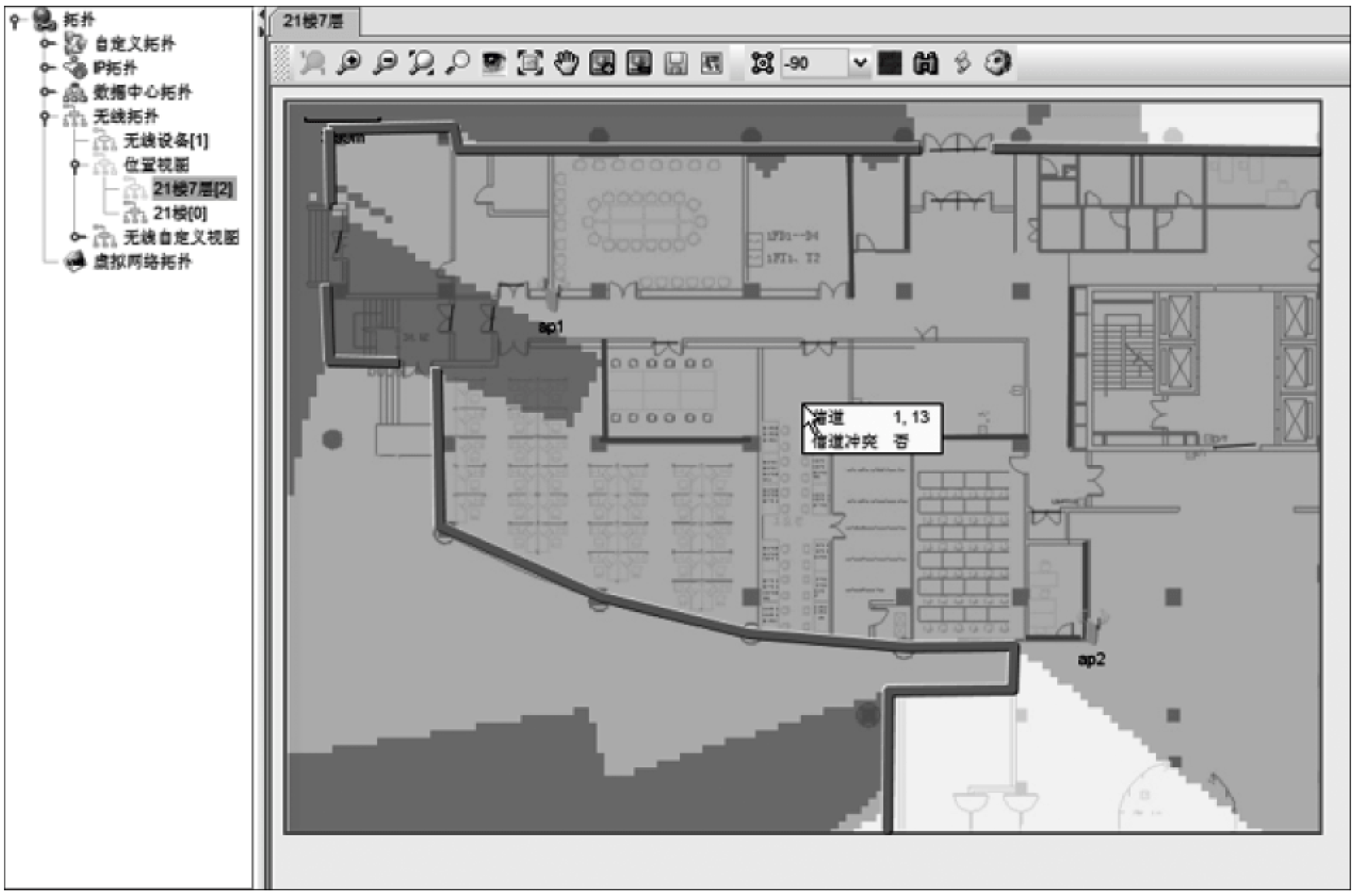


图 8-194 显示信道冲突情况

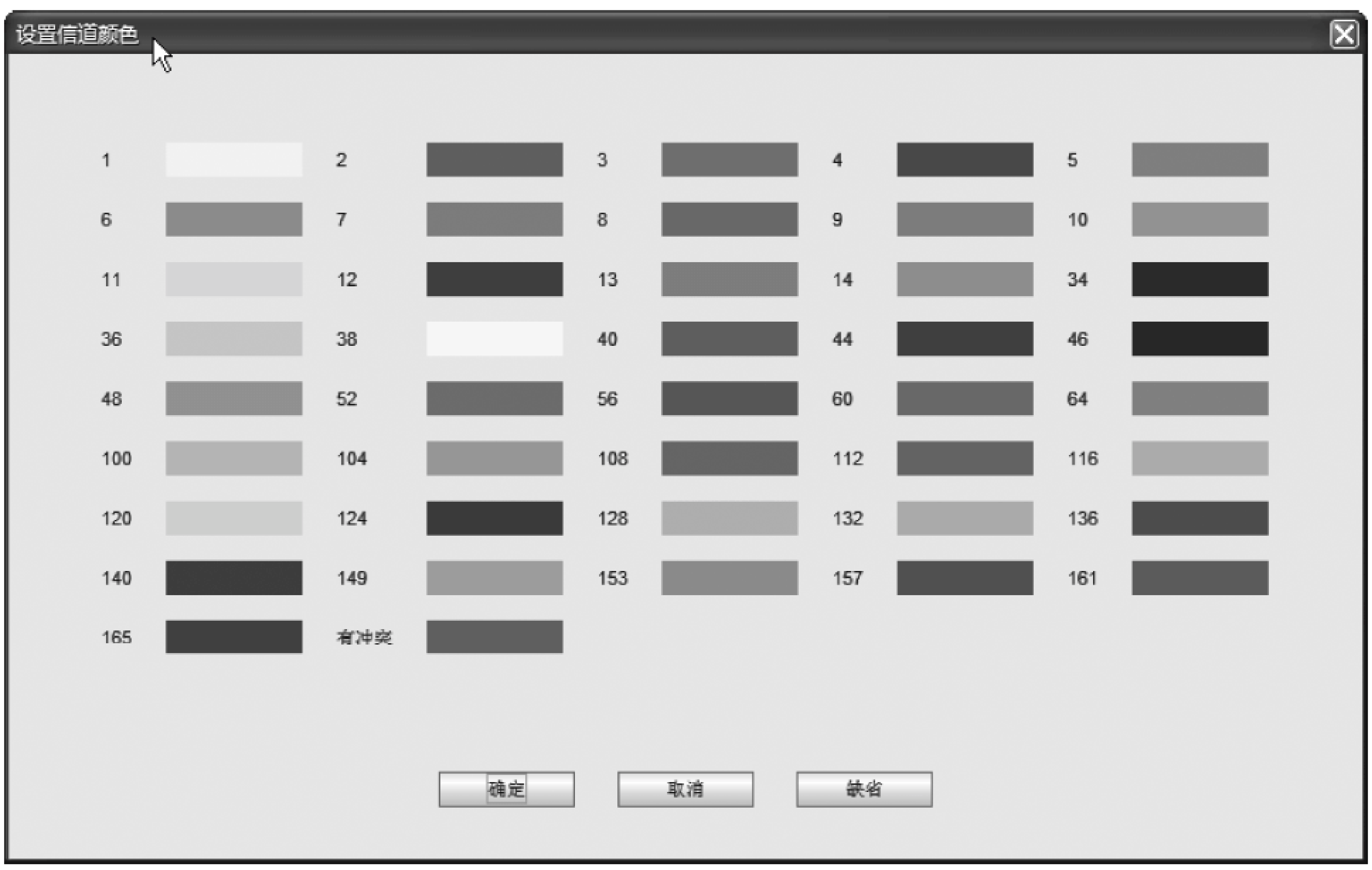


图 8-195 “设置信道颜色”对话框

⑤ 检查显示信号覆盖范围。

具体检查配置的步骤如下。

① 检查位置视图是否按照如下步骤创建并配置。

选择“业务”标签，单击无线业务管理导航树中的“视图管理”菜单组中的“位置视图”命令，进入位置视图管理页面。

单击“增加”按钮，进入增加位置视图页面，如图 8-196 所示。



图 8-196 增加位置视图页面

输入位置名，如“虚拟 AP 举例”，选择位置类型；选择是否热点；如果选择是热点，设置热点扩展属性。

说明：

(a) 位置类型包括以下 4 种类型：区域、楼宇、楼层和房间，增加位置视图时默认为“区域”类型。“区域”类型的位置视图可以增加任意类型的子位置视图；“楼宇”类型的位置视图只能增加“楼层”和“房间”类型的子位置视图；“楼层”类型的位置视图只能增加“房间”类型的子位置视图；“房间”类型的位置视图不能增加子位置视图。

(b) 设置为热点的位置视图不能增加子位置视图。

单击“确定”按钮，完成增加位置视图，如图 8-197 所示。



图 8-197 完成增加位置视图

单击“虚拟 AP 举例”行的“查看拓扑”链接，打开位置视图拓扑，如图 8-198 所示。

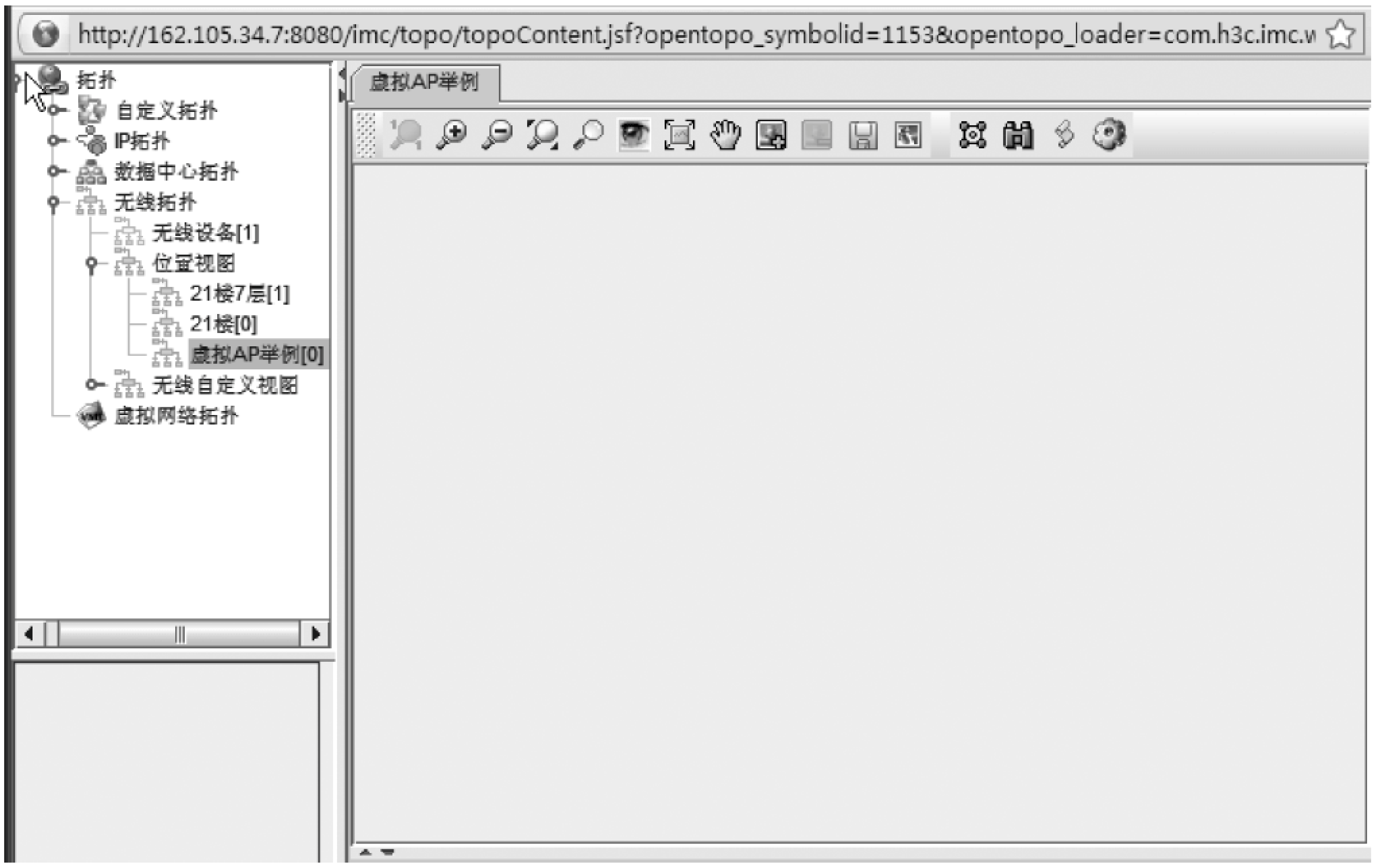


图 8-198 “查看拓扑”链接

在位置视图拓扑工具栏中单击“添加背景图”按钮，选择背景图片，并单击“设置”按钮，如图 8-199 所示。

说明：设置拓扑背景图有两种方式：“用户上传背景图片”和“从背景图库中选择”，“用户上传背景图片”使用过的背景图片自动加入图库，支持的图片格式、大小、尺寸等要求见页面提示。

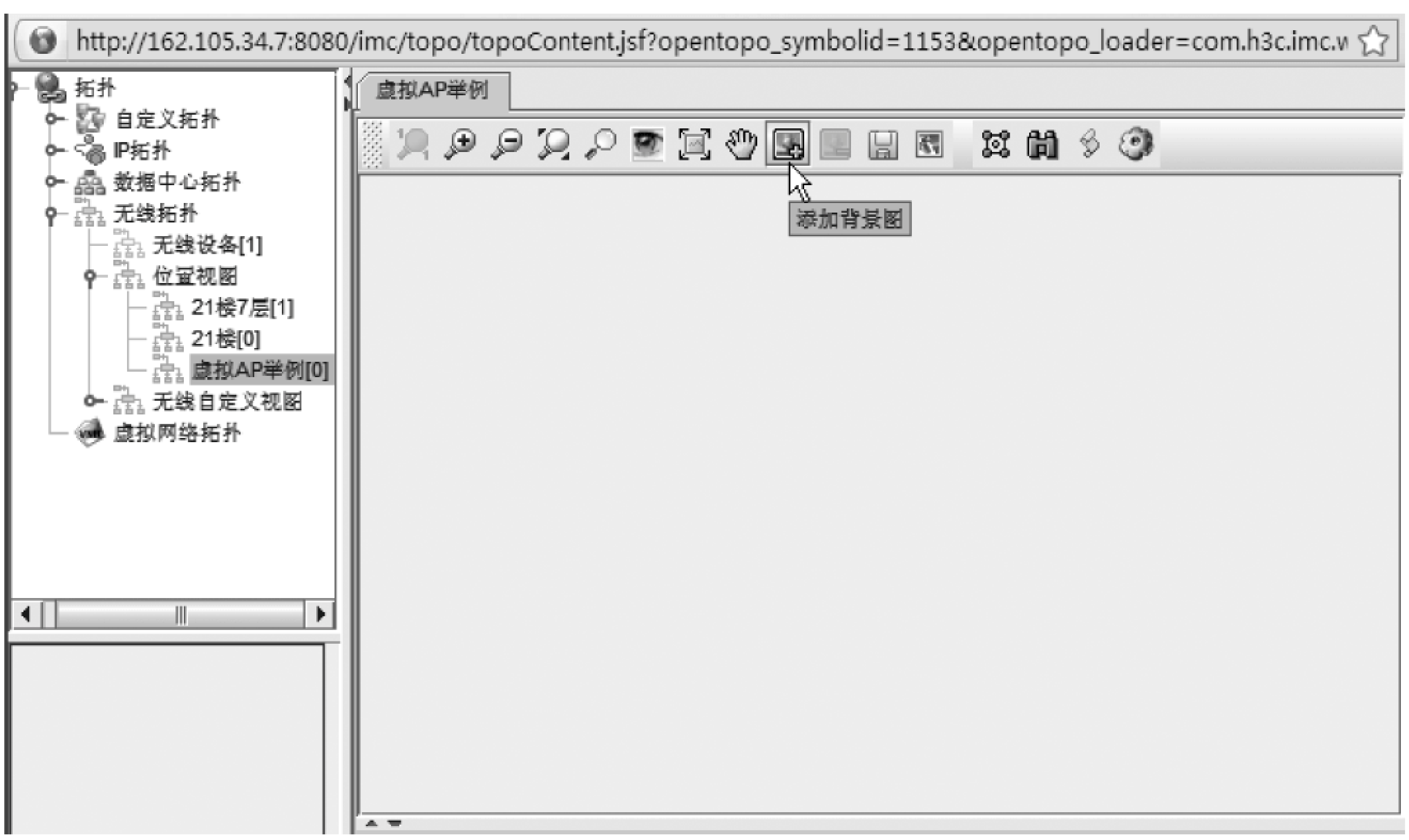


图 8-199 添加背景图

选择背景图，如图 8-200 所示。

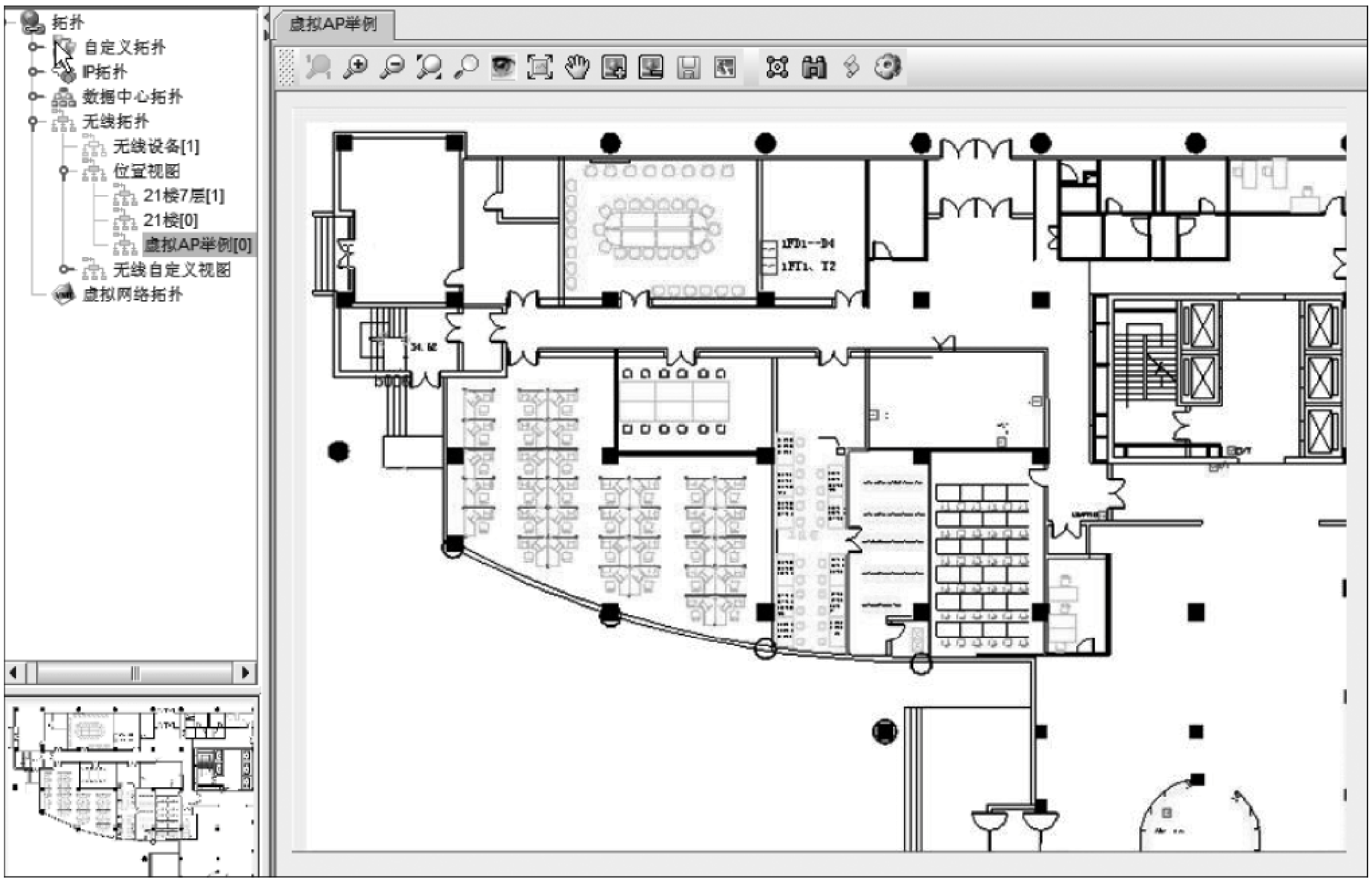


图 8-200　选择背景图

单击右键菜单中的"设置比例尺"菜单，按住鼠标左键，在背景图的两点之间画一条线，放开鼠标左键，在弹出的"指定实际长度"对话框中指定这两点间的实际长度，单位为米，如图 8-201 所示。

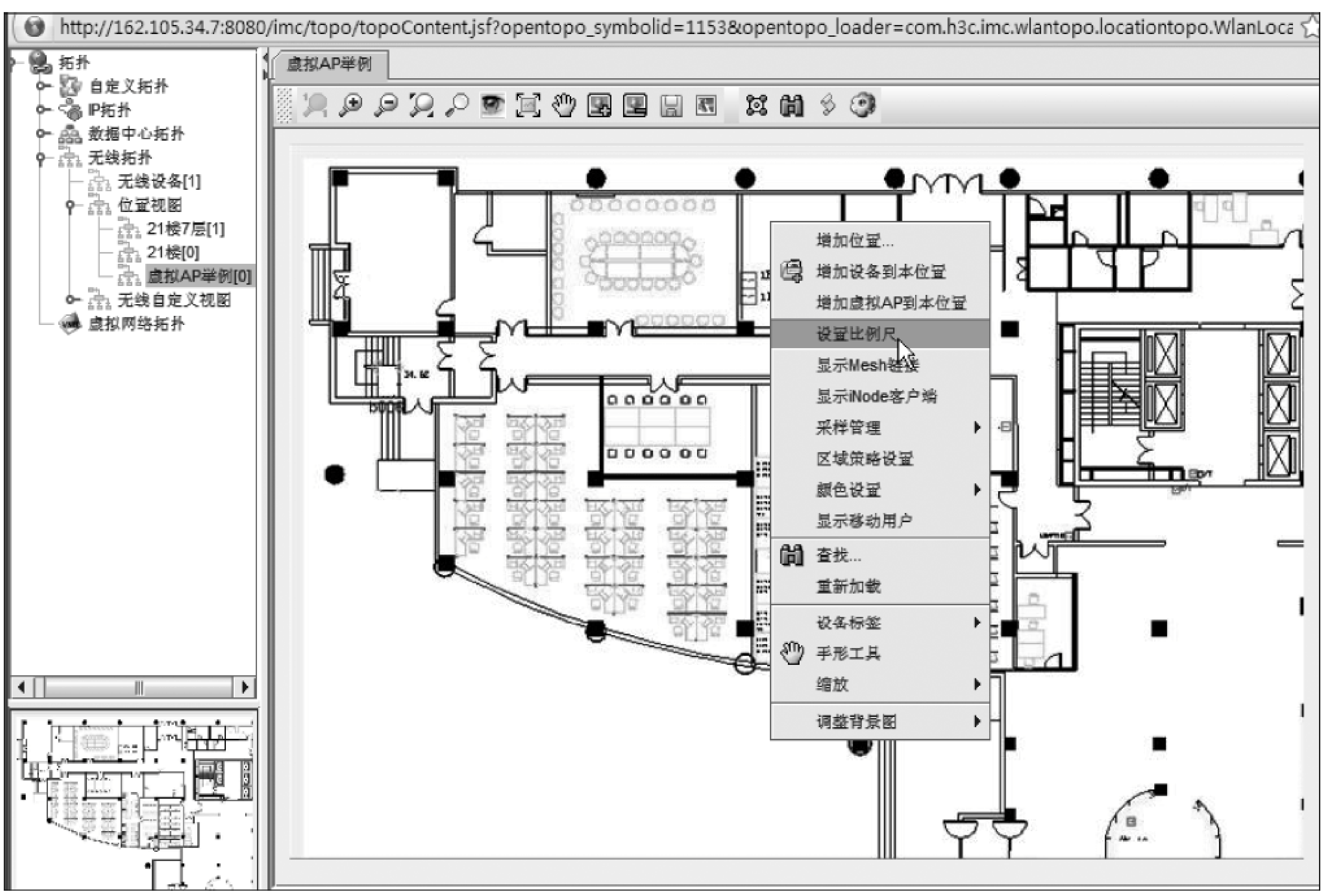


图 8-201　设置比例尺

“指定实际长度”设置，如图 8-202 所示。



图 8-202 “指定实际长度”对话框

如果实际位置视图环境中存在障碍物，单击工具栏中的“增加障碍物”按钮增加障碍物，如图 8-203 所示。

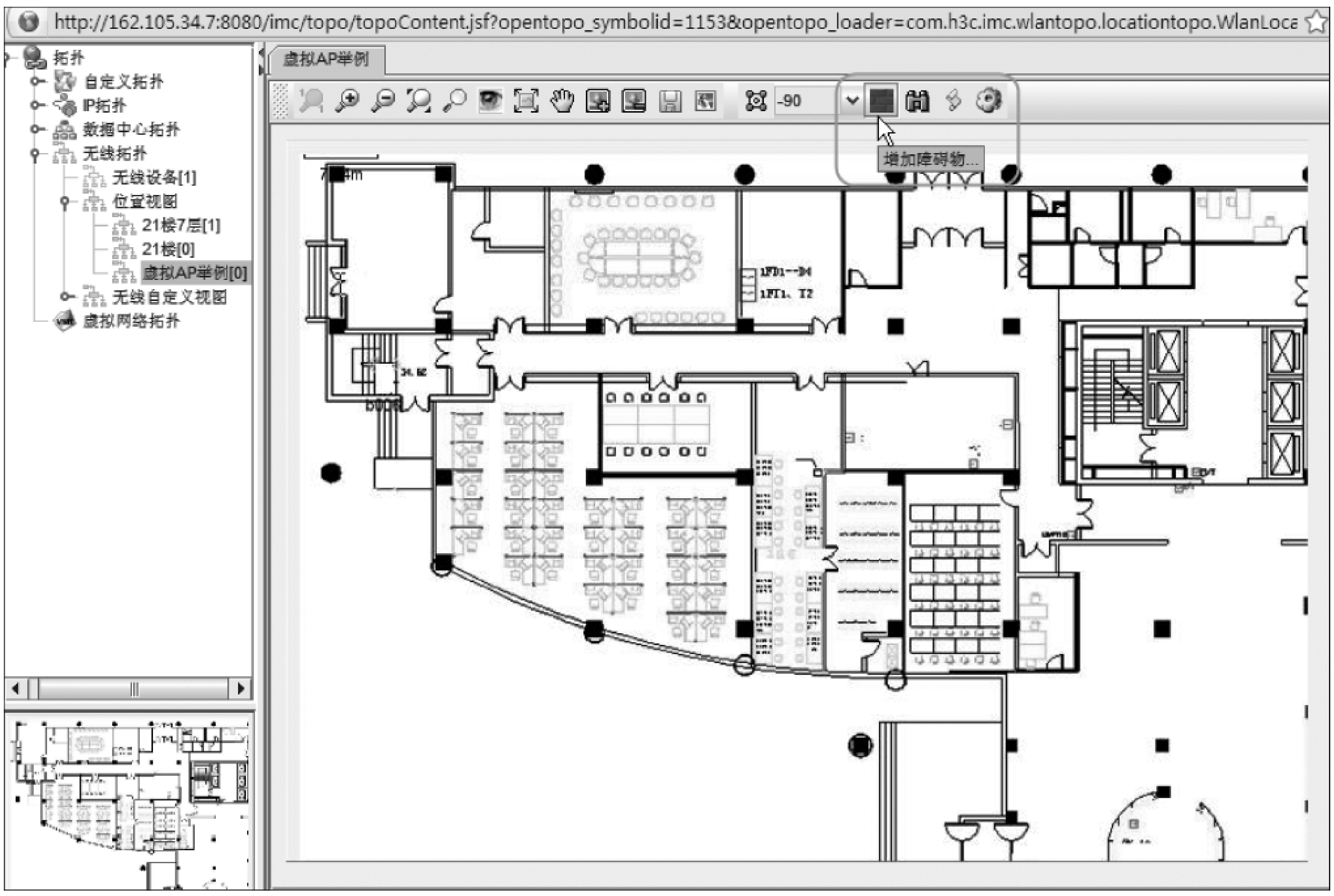


图 8-203 增加障碍物

在“增加障碍物”对话框中选择合适的形状、类型，指定厚度，单击“确定”按钮开始增加障碍物，如图 8-204 所示。



图 8-204 “增加障碍物”对话框

设置障碍物后，根据实际增加障碍物，增加完成后，单击“指针工具”按钮结束增加，如图 8-205 所示。

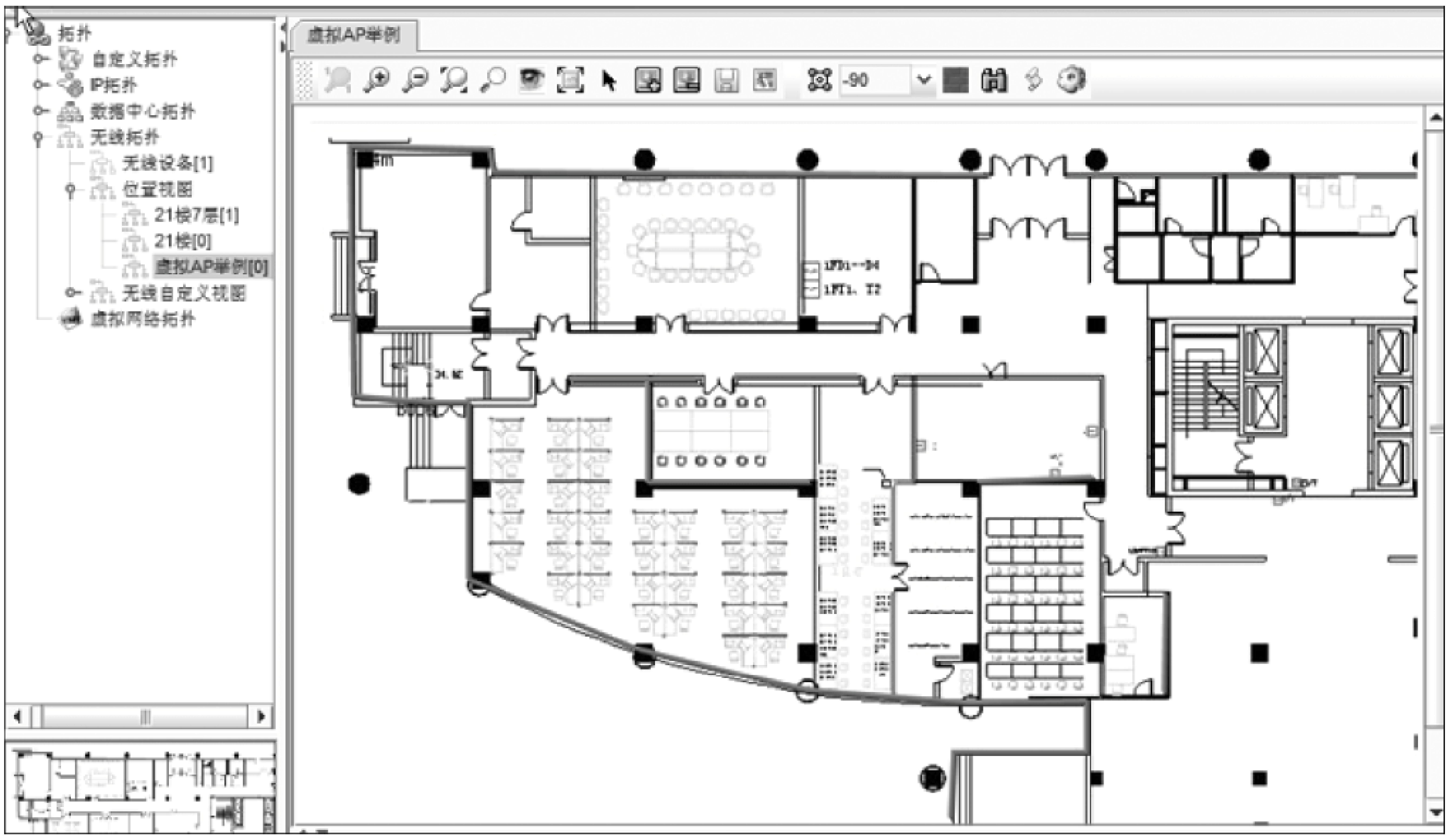


图 8-205　结束增加障碍物

② 检查是否增加并正确设置了虚拟 AP。

在位置视图拓扑中，单击右键菜单中的“增加虚拟 AP 到本位置”命令，如图 8-206 所示。

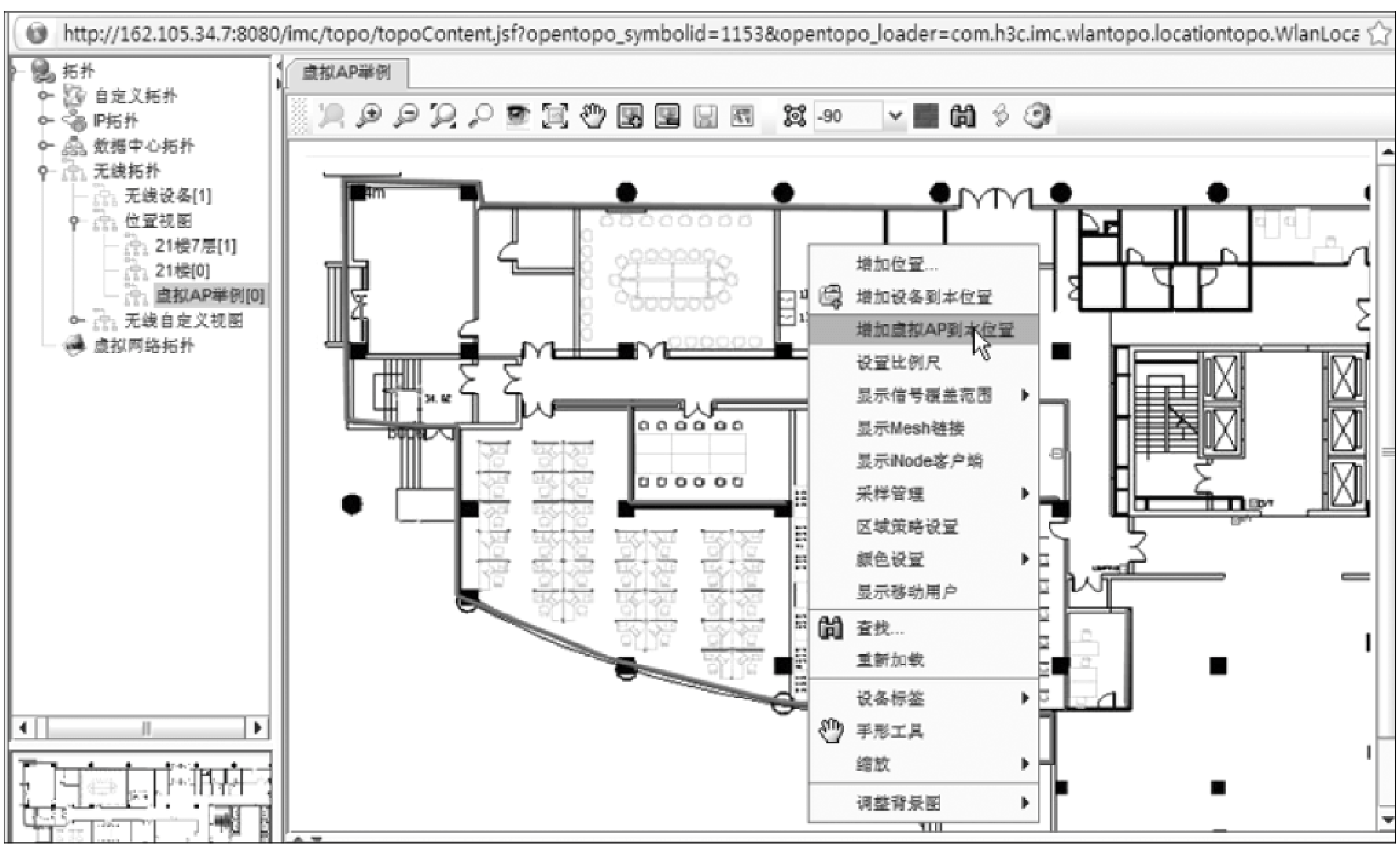


图 8-206　“增加虚拟 AP 到本位置”菜单

在弹出的“选择 AP 型号”对话框中选择要增加的 AP 型号，单击“确定”按钮，如图 8-207 所示。

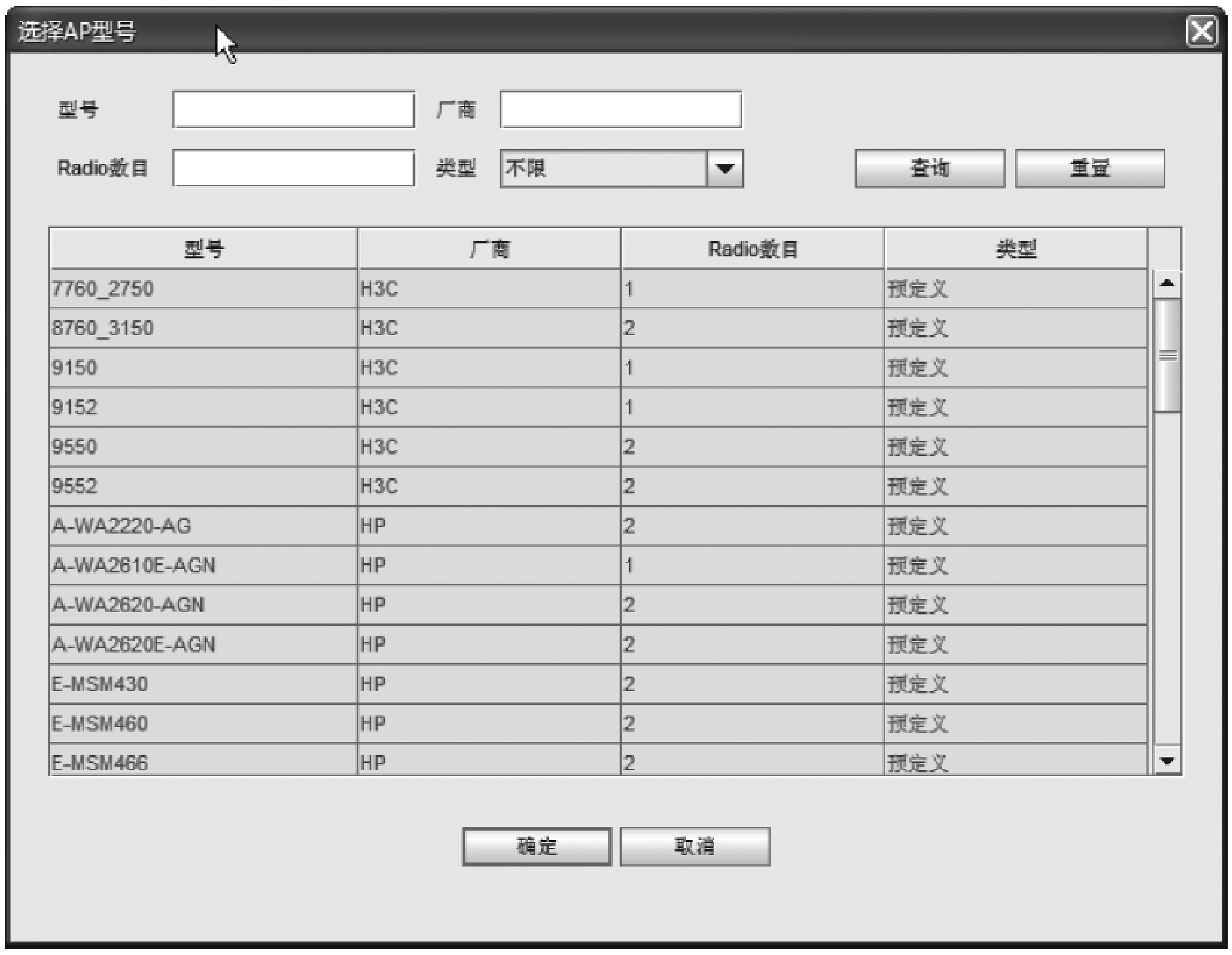


图 8-207 “选择 AP 型号”对话框

在背景图上打算放置 AP 的地方单击鼠标左键放置虚拟 AP，按 Esc 键结束，如图 8-208 所示。

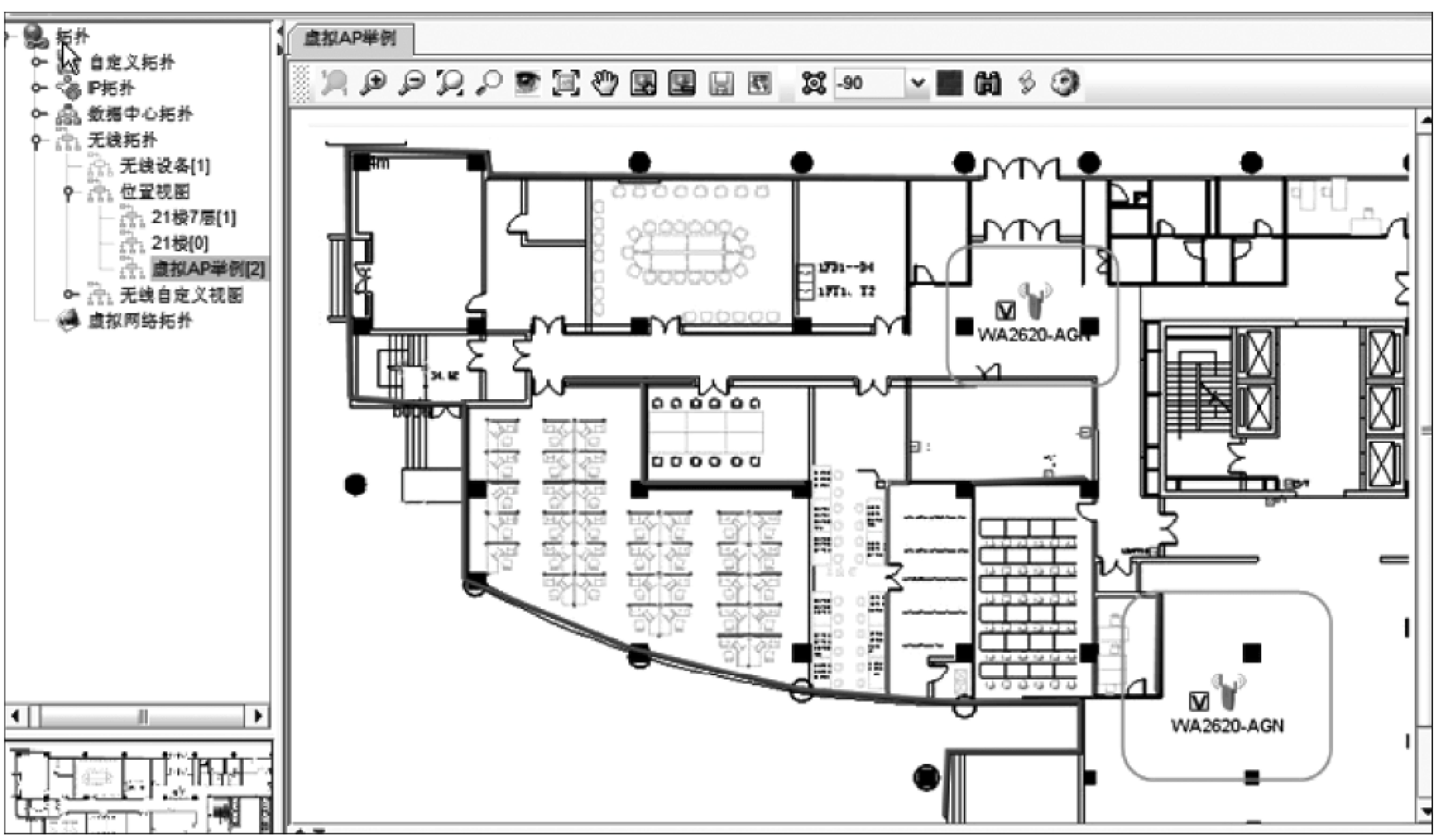


图 8-208 按 Esc 键结束

在虚拟 AP 上单击右键，单击菜单中的“修改虚拟 AP”命令，如图 8-209 所示。

在“修改虚拟 AP”对话框设置 AP 名称，Radio 类型、信道、功率以及天线和角度等信息后，单击“确定”按钮，如图 8-210 所示。

设置完虚拟 AP 参数后，单击“保存”按钮。

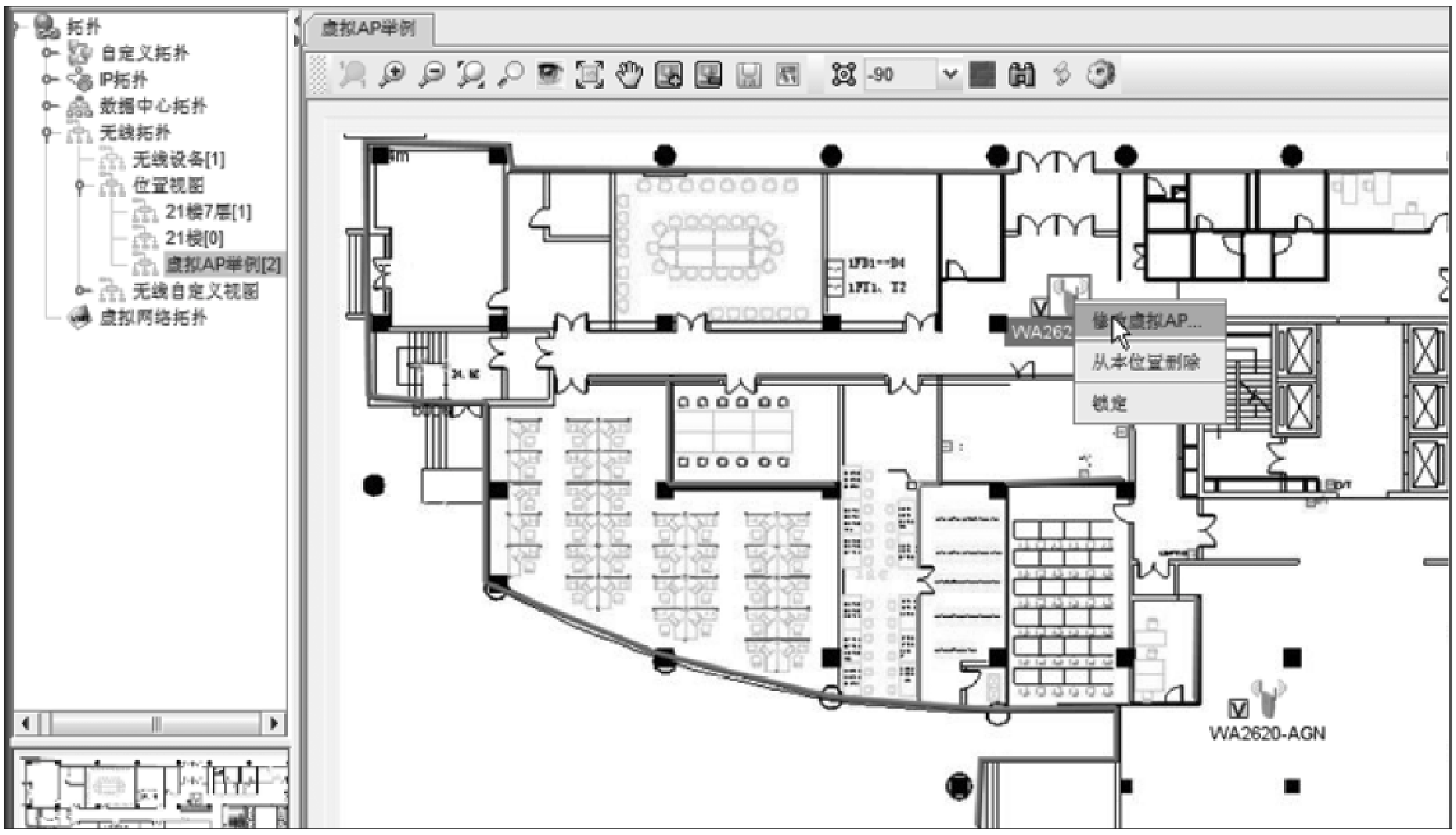


图 8-209　“修改虚拟 AP”菜单

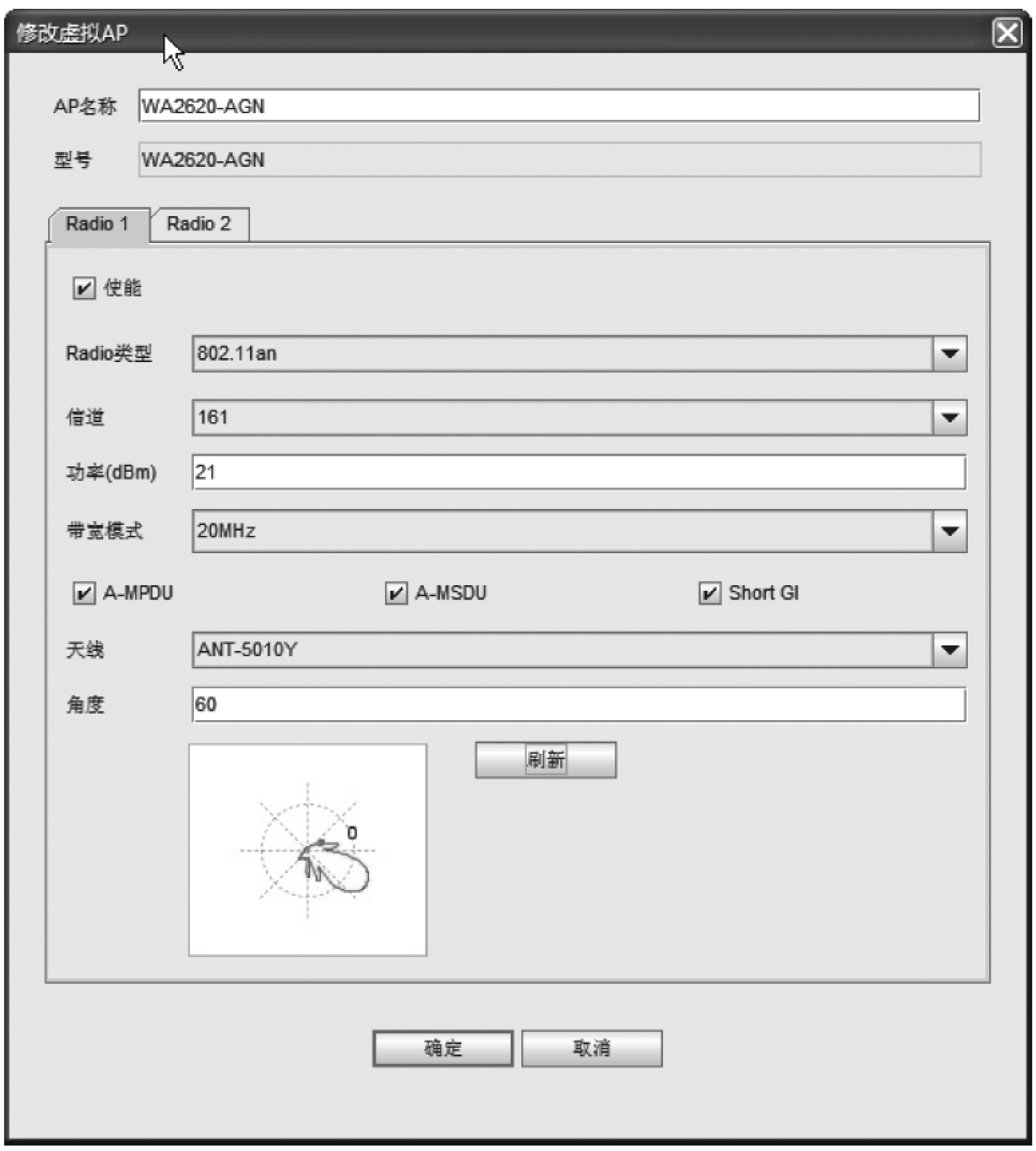


图 8-210　“修改虚拟 AP”对话框

③ 检验配置结果，查看信号覆盖范围。

在位置视图拓扑中，单击右键菜单中的“显示信号覆盖范围”中的命令，如图 8-211 所示。

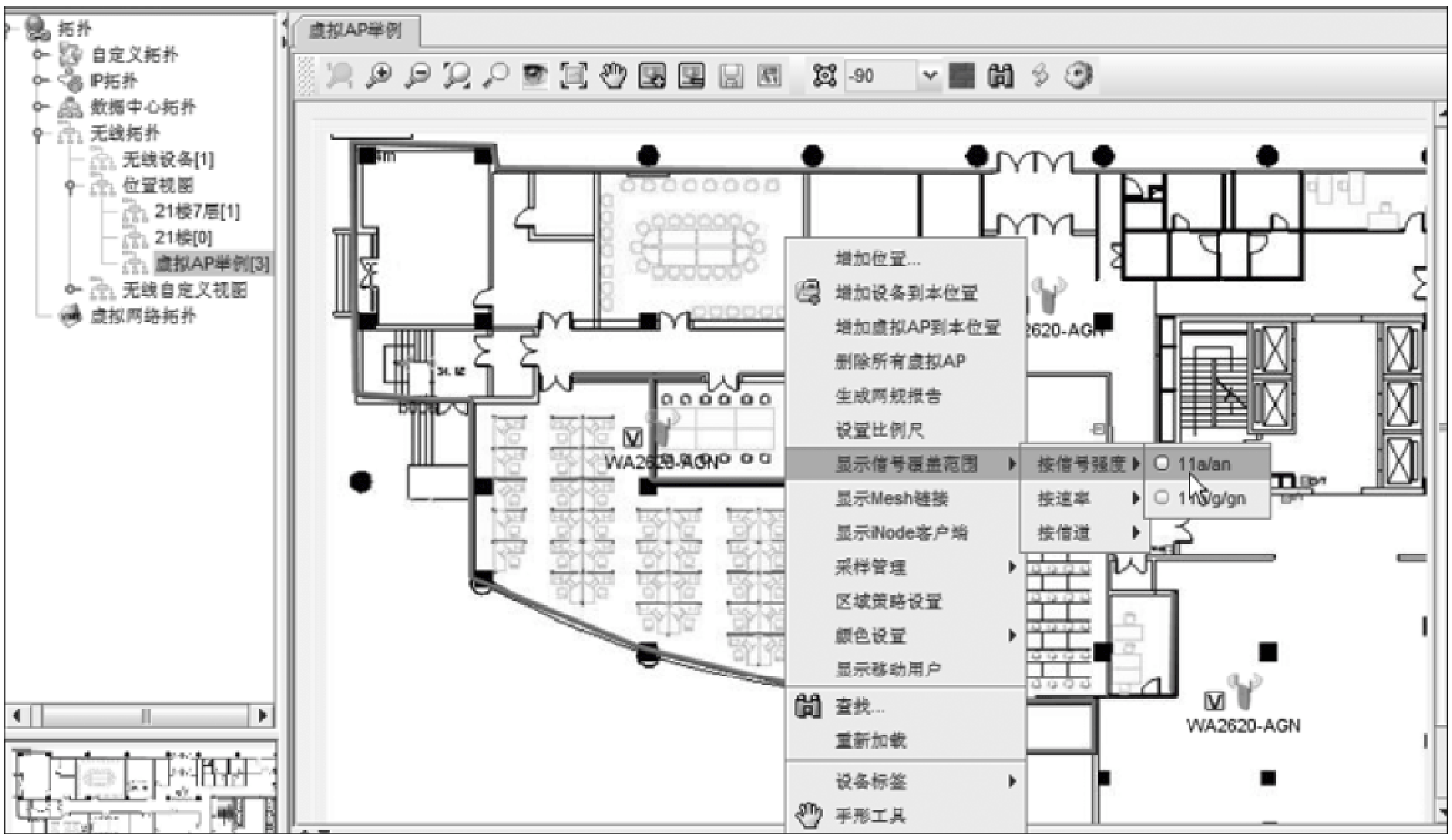


图 8-211 “显示信号覆盖范围”菜单

按信号强度显示信号覆盖范围，单击鼠标左键可以显示该处的信号强度。单击工具栏中的“接收灵敏度”按钮可以修改查看的最低信号强度，如图 8-212 所示。

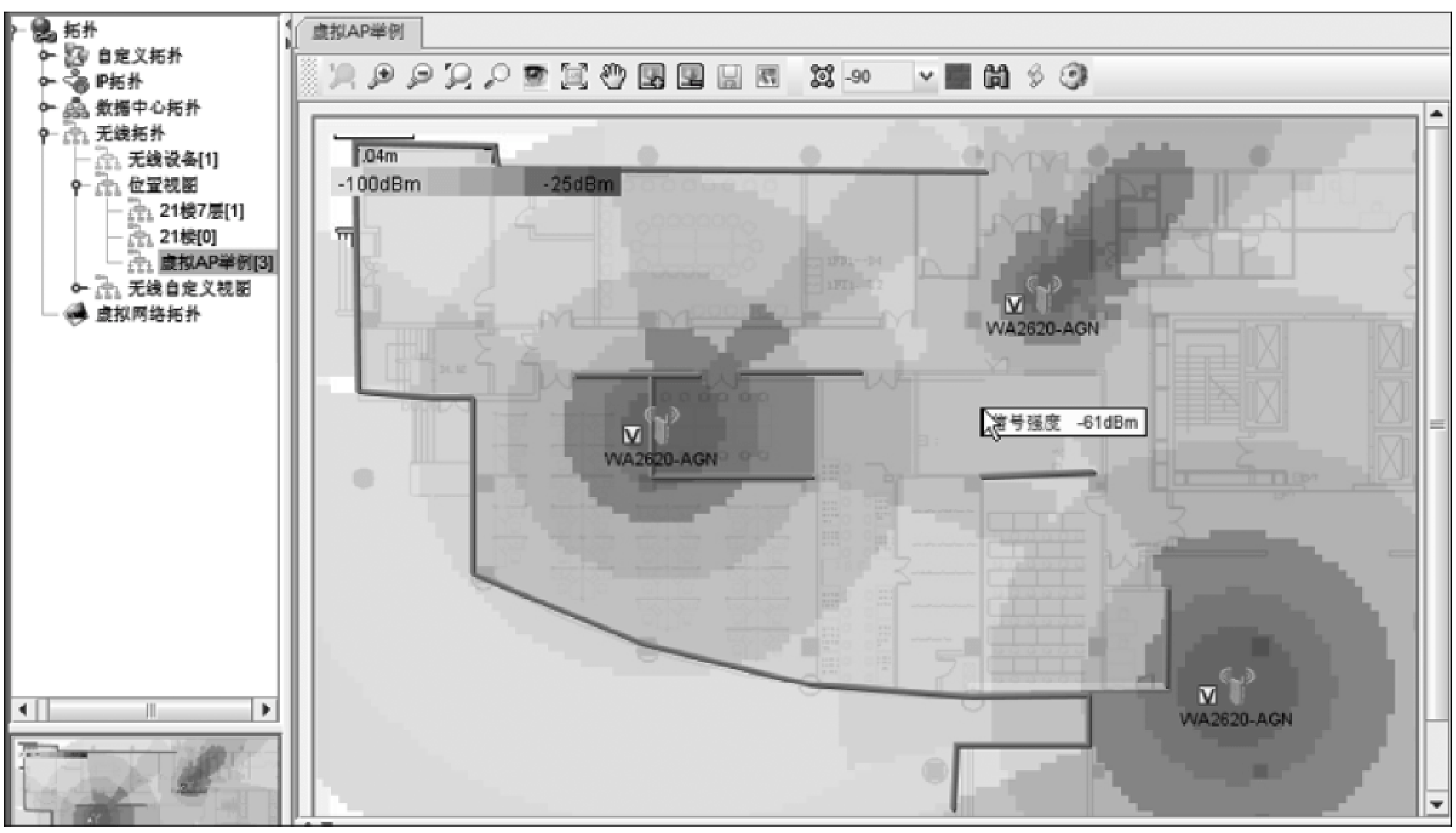


图 8-212 查看最低信号强度

按速率显示信号覆盖范围，单击可以显示该处的速率，如图 8-213 所示。

按信道显示信号覆盖范围，单击可以显示该处的信道冲突情况。对于有信道冲突的区域，可调整 AP Radio 的功率和信道等配置后再次查看信号覆盖范围。对于有信道重叠的区域，

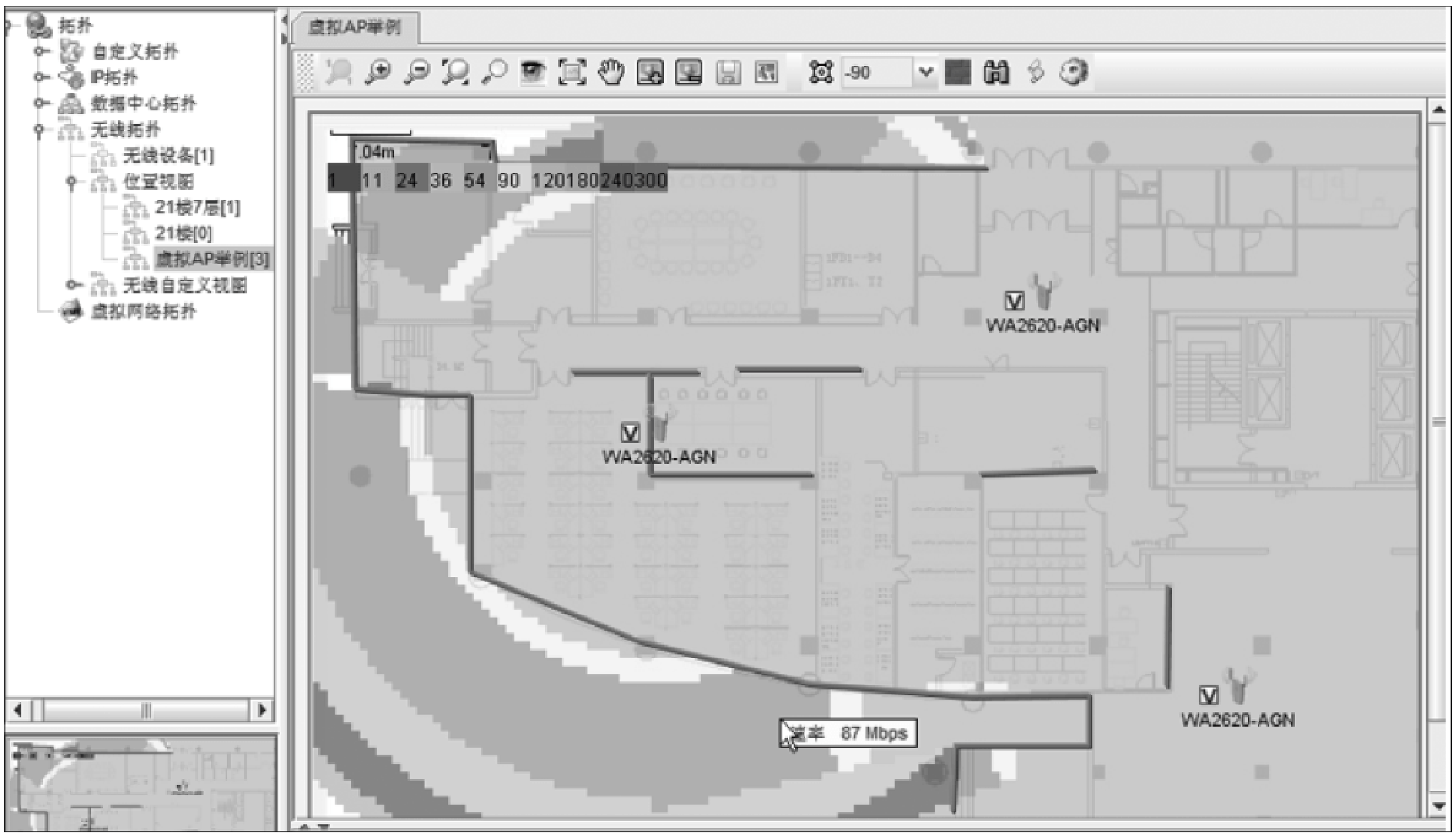


图 8-213 显示速率

颜色也有响应的叠加颜色效果，如图 8-214 所示。



图 8-214 显示信道冲突情况

说明：对于有信号盲点或信道冲突的区域，可再次调整 AP 位置，Radio 的功率和信道等配置后再次查看信号覆盖范围。


iMC APM 数据库管理故障排查
王树旺
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
APM与监控对象可达性检查
检查监控的数据库类型
ORACLE
SQL Server
MySQL
DB2
SYBASE
达梦数据库
Informix
监控对象配置检查
注意事项检查
版本已知问题排查
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC APM(应用管理)产品主要应用于企业数据中心网络，对数据中心涉及应用服务器、数据库、操作系统、邮件服务器、Web 服务器、服务等应用进行数据采集和监控。在应用监控的基础上，结合告警、报表等功能，对网络中的所有应用进行可用性和健康度评价，帮助网络管理员了解网络应用的运行状况，并及时发现网络应用的隐患。APM 数据库管理作为数据中心重要的功能之一，可以对 Oracle、MySQL、SQL Server、DB2、SysBASE 等主流数据库的详细监控。

iMC APM 数据库管理故障的定位思路：首先检查服务器软硬件及性能是否满足当前需要以及 iMC 相应进程运行及数据库连接是否正常，然后检查 APM 服务器和监控对象的连通性，再根据监控的具体数据库类型分别对 APM 监控对象的配置及相关参数的配置进行统一排查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，是否需要分布式。重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

(2) iMC 服务器运行情况检查

单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查 APM 功能组件是否部署成功，进程是否正常运行。

① 检查是否已经部署平台的告警和性能模块。

iMC APM 强依赖 iMC PLAT 的告警和性能功能模块，故必须先安装部署好平台的告警和性能模块后，才能安装部署 iMC APM 业务组件，如图 8-215 所示。



图 8-215 检查是否已经部署平台的告警和性能模块

APM 和平台的版本有相应配套要求，具体请参考 APM 的版本说明书。

② 检查是否已经正常安装部署 APM 业务组件，如图 8-216 所示。

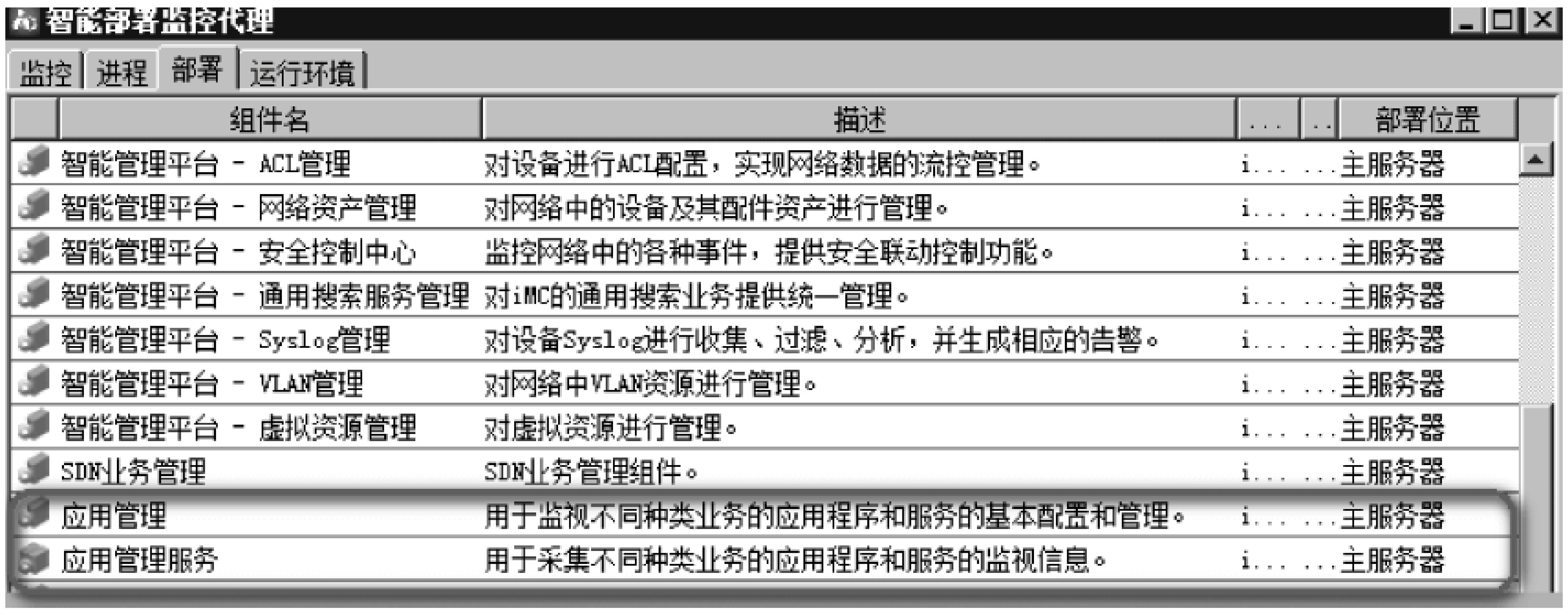


图 8-216　检查是否已经正常安装部署 APM 业务组件

(a) 应用管理：即 APM 的配置模块及前台模块。

(b) 应用管理服务：负责 APM 应用采集，该模块可分布式多次来降低 APM 服务器的集中压力，而应用管理只能部署一次。

③ 检查数据库服务是否运行正常。

以 SQL Server 2008 R2 举例。

单击“开始”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在弹出如图 8-217 所示对话框中，检查各服务的状态是否“正在运行”。

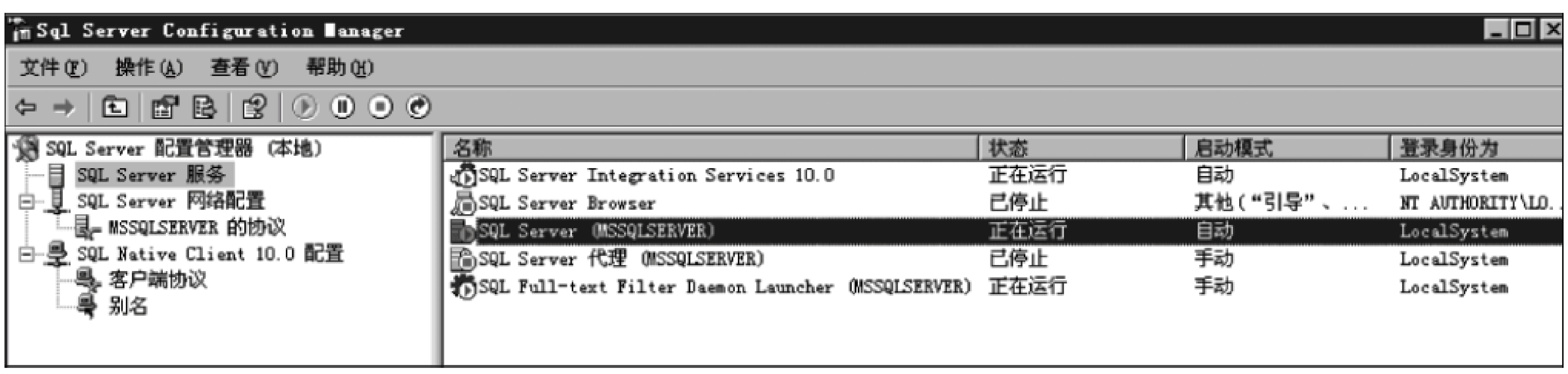


图 8-217　“Sql Server Configuration Manager”对话框

说明：

(a) SQL Server(MSSQL SERVER)是 SQL 的最主要服务，必须处于“正在运行”状态。

(b) iMC 要求 SQL Server(MSSQLSERVER)服务必须以 LocalSystem 身份登录。

④ 检查数据库的相关参数配置是否正确。

⑤ 检查 TCP/IP 参数。

以 SQL Server 2008 R2 举例。

单击“开始”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在弹出如下对话框中，单击左侧树上的“SQL Server 网络配置”→“MSSQLSERVER 的协议”命令，在右侧界面中，双击“TCP/IP”打开“TCP/IP 属性”配置对话框，如图 8-218 所示。

在“协议”标签中确认“全部侦听”为“是”，如图 8-219 所示。

在“IP 地址”标签下，确认各个 IP 地址下的“已启用”为“是”，“TCP 端口(TCP Port)”为“1433”，如图 8-220 所示。



图 8-218　“TCP/IP 属性”配置对话框

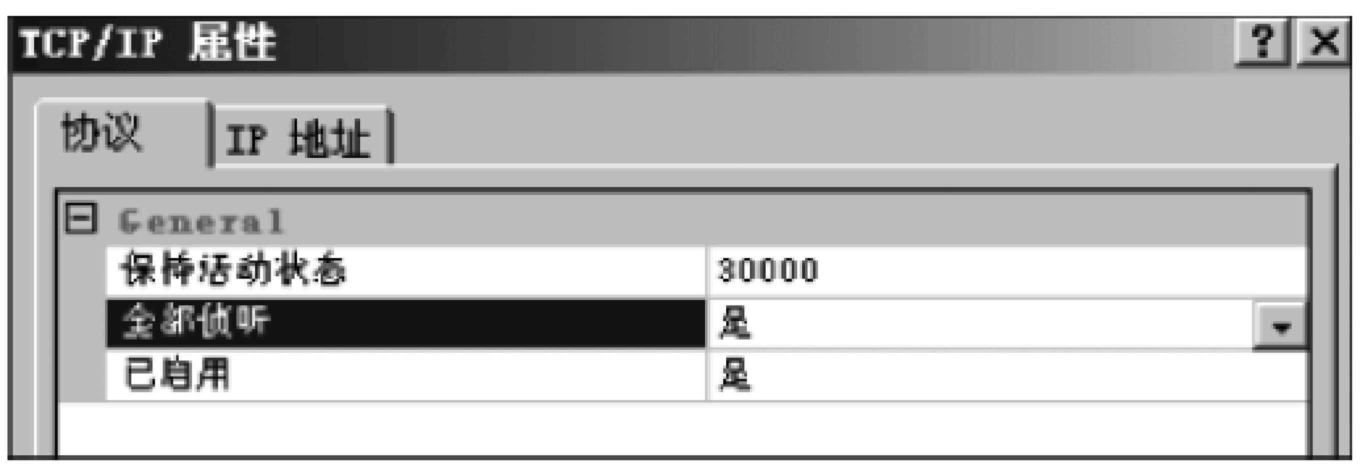


图 8-219　“协议”标签

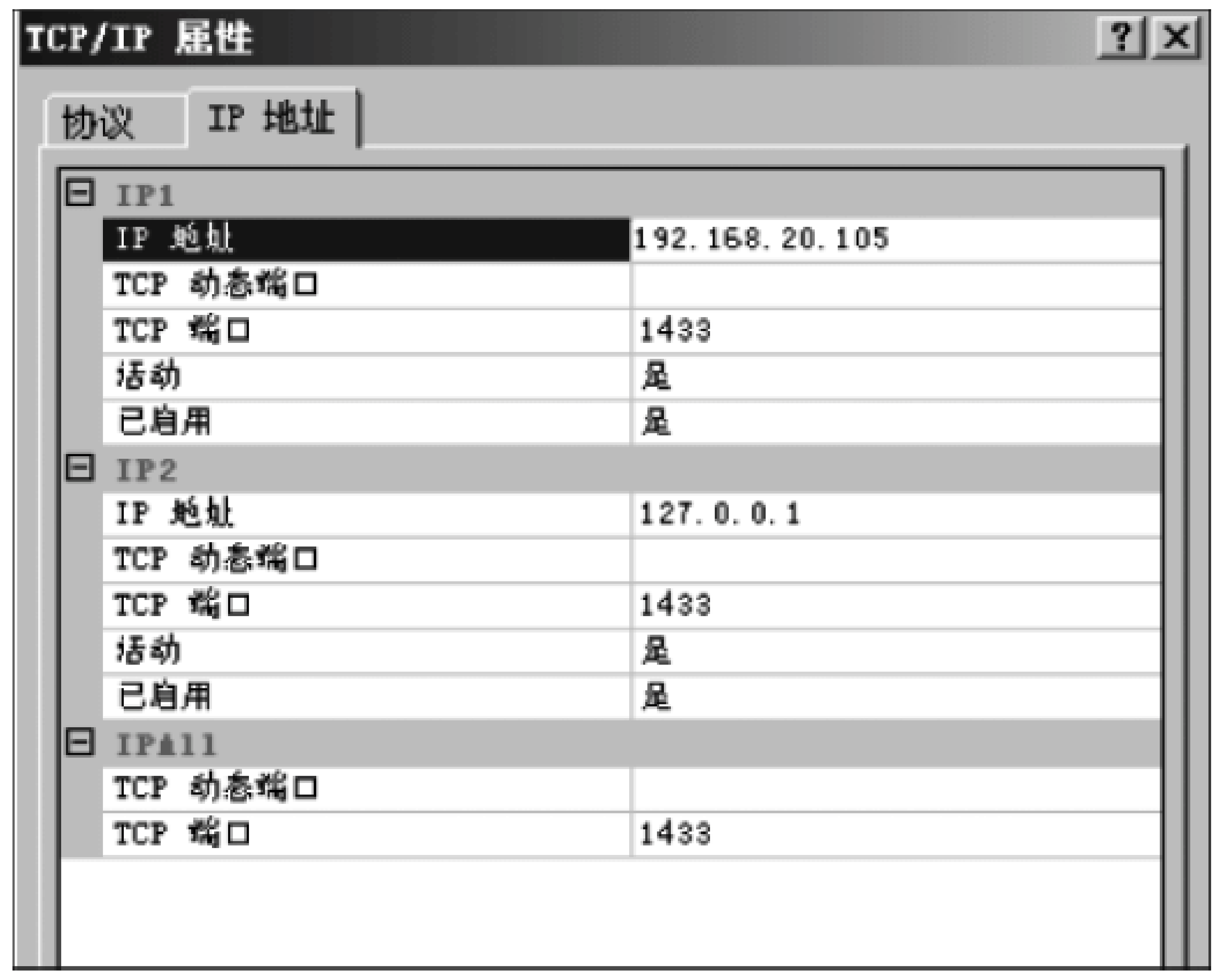


图 8-220　“IP 地址”标签

说明：

(a) 如果前面“TCP/IP 属性”配置界面中，没有将“全部侦听(Listen All)”的值改为“是(Yes)”，则在 SQL Server 2008 R2 安装完成后，如果服务器的 IP 地址更改了，必须重新进入该配置窗口，将原来配置的“IP 地址(IP Address)”进行更新，否则无法连接数据库。

(b) 同样方法确认 Named Pipes 属性也被使能。

(c) 在分布式部署场景中，如果使用了多个数据库服务器，各服务器的监听端口必须相同。

⑥ 检查 SQL Server 的登录方式。

单击“开始”→“程序”→“Microsoft SQL Server 2008 R2”→“配置工具”→“SQL Server 配置管理器”命令，在如图 8-221 所示对话框中查看 SQL Server 服务的“登录身份为”列，确保其值为“LocalSystem”。

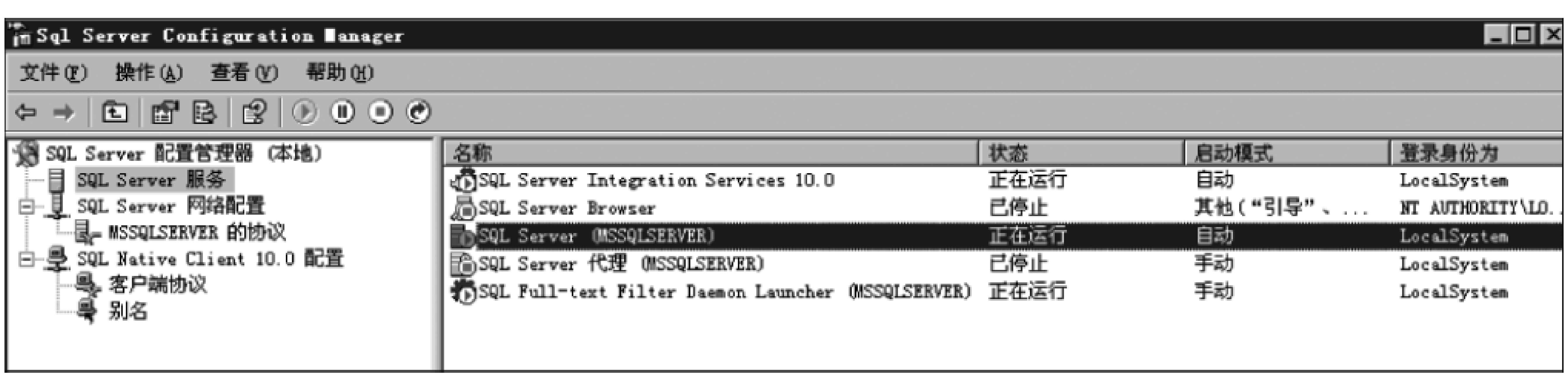


图 8-221　查看 SQL Server 服务

如果当前不是以“LocalSystem”身份登录，需要将其改为“LocalSystem”。双击该行(或选中该行后，单击工具栏中的“属性”按钮)，打开“SQL Server 属性”配置对话框，将“登录身份

为”改为“内置账户”中的“本地系统(LocalSystem)”,如图 8-222 所示。



图 8-222 “SQL Server 属性”对话框

⑦ 检查部署监控代理数据库显示状态。

单击“开始”→“智能部署监控代理”命令,选择“运行环境”标签,正常情况如图 8-223 所示,能正常显示数据库空间使用情况。

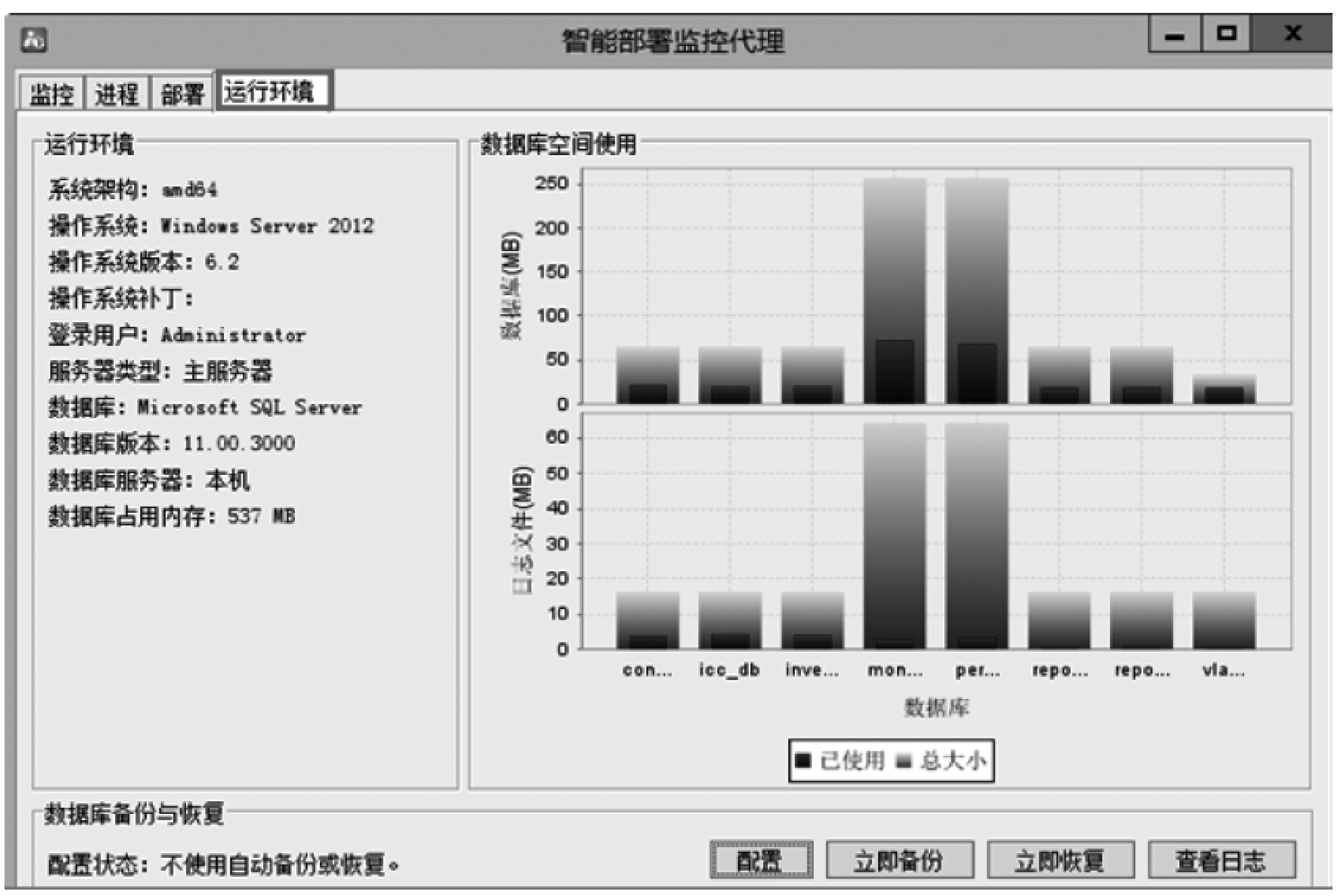


图 8-223 “运行环境”标签

(3) 检查 iMC APM 和数据库的连通情况

APM 要监控数据库的前提是必须确保 APM 和监控对象能正常通信,可以在 APM 服务器的 CMD 命令行通过 ping 命令测试和监控对象是否能正常通信。

(4) 确认监控对象的类型

iMC APM 当前可以管理 Oracle、SQL Server、DB2、MySQL、SysBASE 5 种数据库,不同的数据库类型其配置方法和故障排查方法有所不同。故在故障排查前,请先和现场人员确认

具体的数据库类型,再参考如下方法逐一排查。

(5) Oracle 数据库排查

① 配置检查。图 8-224 所示为 Oracle 数据库排查配置检查。



图 8-224　Oracle 数据库排查配置检查

(a) 数据库主机 IP 地址检查:即数据库所在主机的 IP。

(b) 应用的名称检查:默认为"应用类型_IP 地址",该参数只具有标识意义,可自己定义。

(c) 应用监控端口检查:该端口非常重要,Oracle 的应用端口默认为 1521,请配置当前应用的实际端口。

(d) 轮询间隔时间检查:该轮询时间,即 APM 读取应用数据的间隔时间,可以根据需要配置具体时间,最小为 1 分钟。

(e) 监视方式检查:分单机和分布式两种,即数据库是否分布式安装,非 APM 数据采集方式。

(f) 数据库实例名检查:即 Oracle 的实例名,必须确保输入了正确的数据库实例名,Oracle 的实例名的获取方法如下。

对于 UNIX/Linux 环境,通过命令 **echo $ORACLE_SID** 查看。

```
#echo $ORACLE_SID
orcl
```

对于 Windows 环境,可以通过两种方法:在 sqlplus 中通过命令:select * from v$instance;查看;查看 Windows 注册表 HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\HOME0\ORACLE_SID 键值。

(g) 用户名检查:请检查 ORACLE 用户名的正确性。

(h) 密码检查:请检查 ORACLE 用户密码的正确性。

② 注意事项检查。iMC APM 对所管理的数据库对象有一定要求,包括支持的监控力度及配置参数要求,在故障排查中,该步骤非常重要,针对 APM 监控 Oracle 数据库对象的限制和要求如下。

(a) APM 支持监控的 Oracle 版本包括 9i、10g 和 11g。

(b) 对 Oracle 进行监控时,需至少具有 Connect 和 Select_Catalog_Role 角色的管理员用户名和密码。

(c) 监视方式中单机模式和分布式模式指的是数据库是否分布式安装,非 APM 数据采集方式。

(6) SQL Server 数据库排查

① 配置检查。图 8-225 所示为 SQL Server 数据库排查配置检查。



图 8-225　SQL Server 数据库排查配置检查

(a) 数据库主机 IP 地址检查:即数据库所在主机的 IP。

(b) 应用的名称检查:默认为“应用类型_IP 地址”,该参数只具有标识意义,可自己定义。

(c) 应用监控端口检查:该端口非常重要,SQL Server 的应用端口默认为 1433,请配置当前应用的实际端口。

(d) 轮询间隔时间检查:该轮询时间,即 APM 读取应用数据的间隔时间,可以根据需要配置具体时间,最小为 1 分钟。

(e) 应用的认证类型检查:分 Windows 认证和 SQL 认证两种。

(f) 用户名检查:认证类型为 Windows 认证时,此用户名为操作系统用户名,否则为数据库名,一般为 sa。

(g) 密码检查:认证类型为 Windows 认证时,此密码为系统密码,否则为数据库密码。

(h) 数据库实例名:如果是 SQL Server 的默认实例,则可以不输入实例名,如果非默认实例,则需要输入实例名。

② 注意事项检查。APM 支持对 SQL Server 2000 SP4、SQL Server 2005 和 SQL Server 2008 的监控。

(7) MySQL 数据库排查

① 配置检查。图 8-226 所示为 MySQL 数据库排查配置数据。

(a) 数据库主机 IP 地址检查:即数据库所在主机的 IP。



图 8-226　MySQL 数据库排查配置数据

(b) 应用的名称检查：默认为“应用类型_IP 地址”，该参数只具有标识意义，可自己定义。

(c) 应用监控端口检查：该端口非常重要，MySQL 的应用端口默认为 3306，请配置当前应用的实际端口。

(d) 轮询间隔时间检查：该轮询时间，即 APM 读取应用数据的间隔时间，可以根据需要配置具体时间，最小为 1 分钟。

(e) 用户名检查：请检查 MySQL 用户名的准确性。

(f) 密码检查：请检查 MySQL 用户的密码的准确性。

② 注意事项检查。

(a) APM 可用监控的 MySQL 版本包括 MySQL 5. x。

(b) 用户必须具有远程访问 MySQL 的权限。

(c) 确认 MySQL 是否可以远程访问方法：登录 MySQL 数据库执行“select host，user from mysql. user”，查看结果中 host 是否包含 APM 服务器地址，如果不包含需要进行授权。

(8) DB2 数据库排查

① 配置检查。图 8-227 所示为 DB2 数据库排查配置检查。

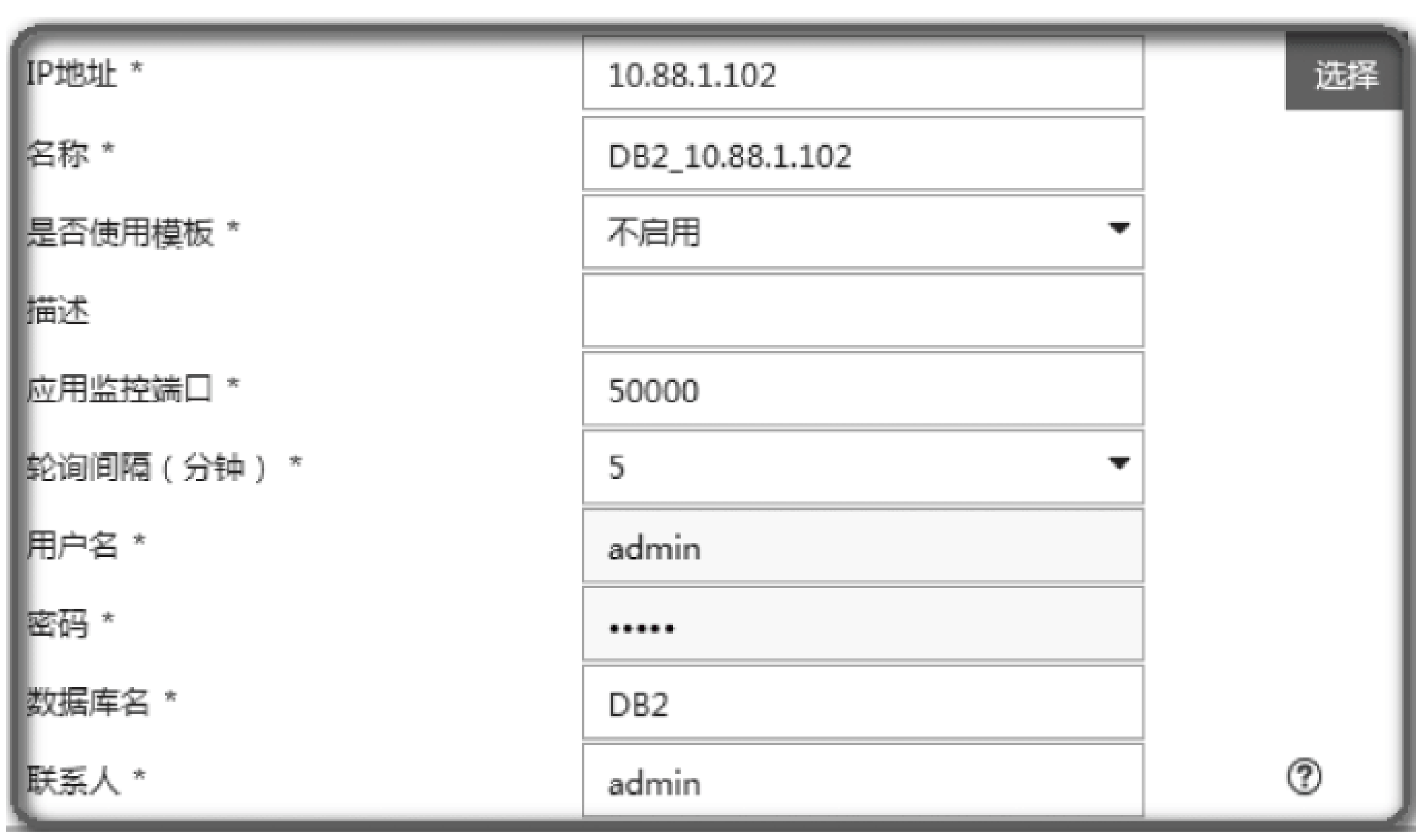


图 8-227　DB2 数据库排查配置检查

(a) 数据库主机 IP 地址检查：即数据库所在主机的 IP。

(b) 应用的名称检查：默认为“应用类型_IP 地址”，该参数只具有标识意义，可自己定义。

(c) 应用监控端口检查：该端口非常重要，DB2 的应用端口默认为 50000，请配置当前应用的实际端口。

(d) 轮询间隔时间检查：该轮询时间，即 APM 读取应用数据的间隔时间，可以根据需要配置具体时间，最小为 1 分钟。

(e) 用户名检查：请检查 DB2 用户名的准确性。

(f) 密码检查：请检查 DB2 用户的密码的准确性。

(g) 数据库名检查：请检查 DB2 数据库名是否正确。

② 注意事项检查。

(a) APM 可以监控 DB2/NT 8.2.0 及以上版本的 DB2。

(b) 对 DB2 进行监控时，需要具有管理员权限的用户名和密码以及数据库名称。

(c) DB2 所有用户都是操作系统用户，要查看数据库与用户名对应关系，在 DB2 控制中心中相应数据库下查看“数据库用户”及其拥有的权限。

(9) SyBASE 数据库排查

① 配置检查。图 8-228 所示为 SyBASE 数据库排查配置检查。



图 8-228　SyBASE 数据库排查配置检查

(a) 数据库主机 IP 地址检查：即数据库所在主机的 IP。

(b) 应用的名称检查：默认为“应用类型_IP 地址”，该参数只具有标识意义，可自己定义。

(c) 应用监控端口检查：该端口非常重要，SyBASE 的应用端口默认为 5000，请配置当前应用的实际端口。

(d) 轮询间隔时间检查：该轮询时间，即 APM 读取应用数据的间隔时间，可以根据需要配置具体时间，最小为 1 分钟。

(e) 用户名检查：请检查 SyBASE 用户名的准确性。

(f) 密码检查：请检查 SyBASE 用户的密码的准确性。

② 注意事项检查。

(a) 可用监控的 SyBASE 版本包括 SyBASE Adaptive Server Enterprise 12.5.2 及以上。

(b) 对 SyBASE 进行监控时，需要具有管理员权限的用户名和密码。

(10) 达梦数据库排查

① 配置检查。图 8-229 所示为达梦数据库排查配置检查。



图 8-229 达梦数据库排查配置检查

(a) 数据库主机 IP 地址检查：即数据库所在主机的 IP。

(b) 应用的名称检查：默认为“应用类型_IP 地址”，该参数只具有标识意义，可自己定义。

(c) 应用监控端口检查：该端口非常重要，达梦数据库的应用端口默认为 5236，请配置当前应用的实际端口。

(d) 轮询间隔时间检查：该轮询时间，即 APM 读取应用数据的间隔时间，可以根据需要配置具体时间，最小为 1 分钟。

(e) 用户名检查：请检查达梦数据库用户名的准确性。

(f) 密码检查：请检查达梦数据库用户的密码的准确性。

② 注意事项检查。

(a) APM 支持监控 DM7 版本。

(b) 对 DM 进行监控时，需要具有数据库管理员权限的用户名和密码。

(11) Informix 数据库排查

① 配置检查。图 8-230 所示为 Informix 数据库排查配置检查。



图 8-230 Informix 数据库排查配置检查

(a) 数据库主机 IP 地址检查：即数据库所在主机的 IP。

(b) 应用的名称检查：默认为“应用类型_IP 地址”，该参数只具有标识意义，可自己定义。

(c) 应用监控端口检查：该端口非常重要，达梦数据库的应用端口默认为 9088，请配置当前应用的实际端口。

(d) 轮询间隔时间检查：该轮询时间，即 APM 读取应用数据的间隔时间，可以根据需要配置具体时间，最小为 1 分钟。

(e) 用户名检查：请检查达梦数据库用户名的准确性。

(f) 密码检查：请检查达梦数据库用户的密码的准确性。

(g) 数据库名检查：请检查数据库名是否正确。

(h) 数据库服务名检查：请检查数据库服务名是否正确。

② 注意事项检查。

(a) APM 可以监控 Informix 9.40 及以上版本的 Informix。

(b) 对 Informix 进行监控时，Informix 在 Linux 上时，Linux 服务器上的配置文件 sqlhosts，主机别名前加 * 。例如：cs_dbs onsoctcp * linux sqlexe。

(c) 对 Informix 进行监控时，用户需要具有管理员权限的用户名和密码以及数据库名称，数据库实例名称。

(12) 版本已知问题排查

早期版本可能存在已知问题或相关使用限制，在 APM 版本说明书中会有说明。在故障排除时，要养成查看版本说明书的习惯。

例如：在 APM 中增加一个 Oracle 数据库监视器，在 iMC 中通过“应用监视”链接查看该应用的详细内容，发现除了第一个 tab 页有数据，后面几个 tab 页都没有内容，如图 8-231 所示。

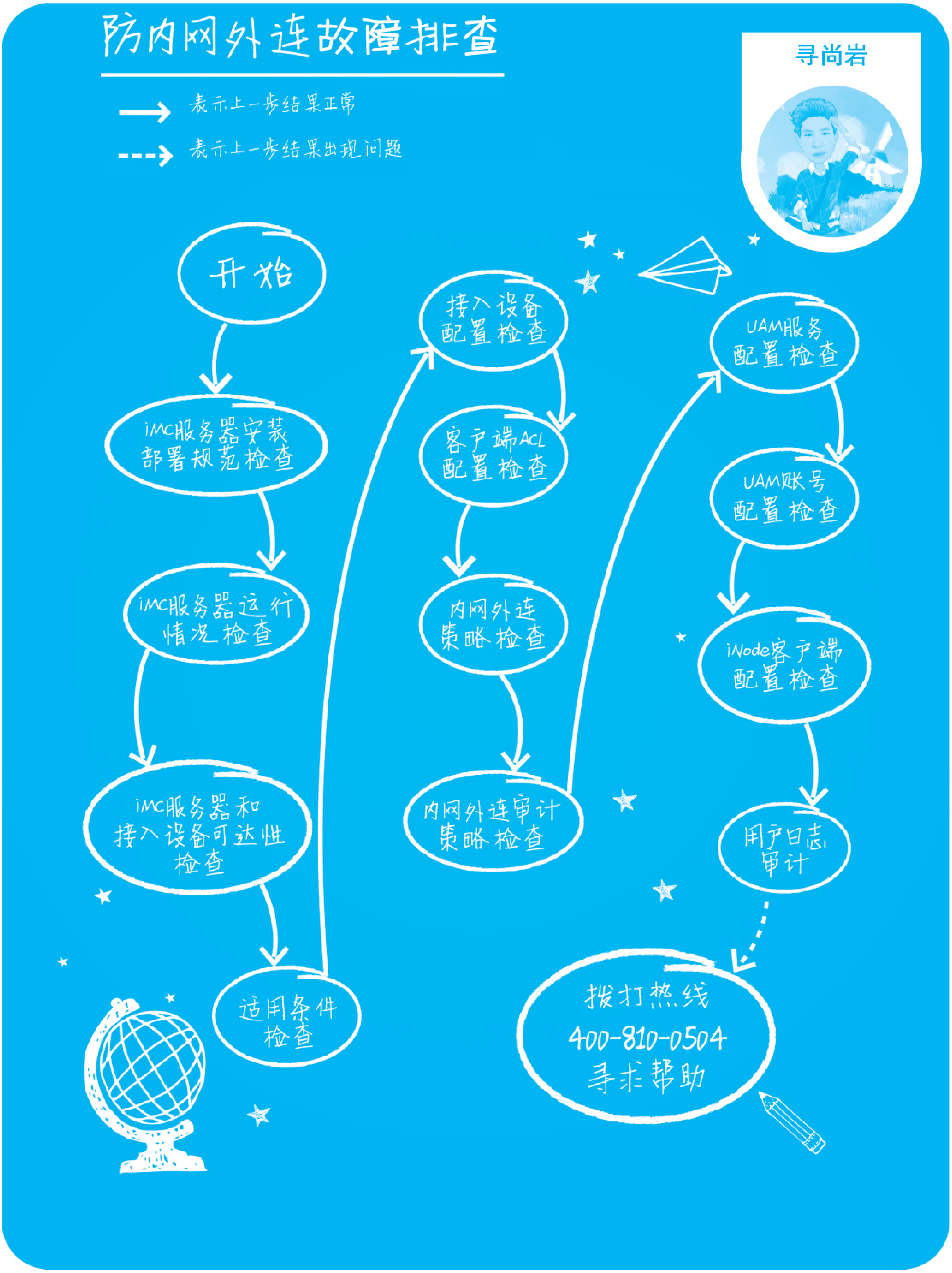


图 8-231 版本已知问题排查

① 存在问题版本。APM 3.20-E0703 之前的版本。

② 原因分析。过滤器类对页面内容进行过滤存在问题，导致页面中内容显示出现问题。

③ 解决方案。安装 APM 3.20-E0703 版本或之后的版本。


防内网外连故障排查
寻尚岩
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和接入设备可达性检查
适用条件检查
接入设备配置检查
客户端ACL配置检查
内网外连策略检查
内网外连审计策略检查
UAM服务配置检查
UAM账号配置检查
iNode客户端配置检查
用户日志审计
拨打热线
400-810-0504
寻求帮助

1. 开始

随着网络的普及，人们接入网络的方式多种多样。比如 PC 可以安装多块网卡，一块网卡进行认证并接受 EAD 控制，另一块网卡则接入了其他网络；或者笔记本电脑等移动终端，除了进行认证外，还可以随时接入其他各种无线网络。很多敏感的网络中，不允许 PC 或笔记本电脑连接多个网络。因此需要一种方法，强制 PC 或笔记本电脑只能接入可信的内网，禁止接入其他网络。H3C iNode 客户端防内网外连功能可以控制用户访问权限，满足阻止用户随意接入网络的需求。PC 接入内网前，客户端防内网外连功能可以将所有网卡置为流出向阻断状态，即所有网卡流出方向只能通过 DHCP 报文，其他所有 IP 报文都被丢弃；流入方向不受限制。只有使用 iNode 客户端在 802.1x 或 Portal 认证成功后，才会将认证网卡完全放开，不过滤任何报文。而除认证网卡外的所有网卡（包括但不限于 Modem、ADSL、GPRS、CDMA 等各种互联网接入）继续处于阻断状态。这样就从源头上严格限制了 PC 对网络的使用，保证了信息安全。对于防内网外连问题定位故障的思路及顺序是：UAM 侧服务器软硬件状态及路由可达性检查、适用条件检查、防内网外连参数配置检查和 iNode 客户端配置检查。

本文举例组网如图 8-232 所示。



图 8-232　组网举例

IP 规划如下。

认证终端 PC：172.16.16.2/24，网关 172.16.16.1。

认证设备：VLAN 16：172.16.16.1/24，VLAN 100：172.16.100.1/24。

iMC 服务器：172.16.100.61/24，网关 172.16.100.1。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题时首先需要确认服务器软硬件配置情况。

请对照《智能管理中心（iMC）部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心（iMC）部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、同时在线人数多，则需要根据《智能管理中心（iMC）部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心（iMC）部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”“策略服务器”“智能策略服务代理”和“安全策略管理前台”组件状态应为“已部署”，如图 8-233 所示。



图 8-233　部署页面

(2) iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程,各进程是否正常为“已经启动”。

① 在部署监控代理中,查看 uam. exe、ispserver、policyserver 进程是否正常启动;如果是 Portal 认证方式还需要确认 portalserver 进程是否正常启动,如图 8-234 所示。

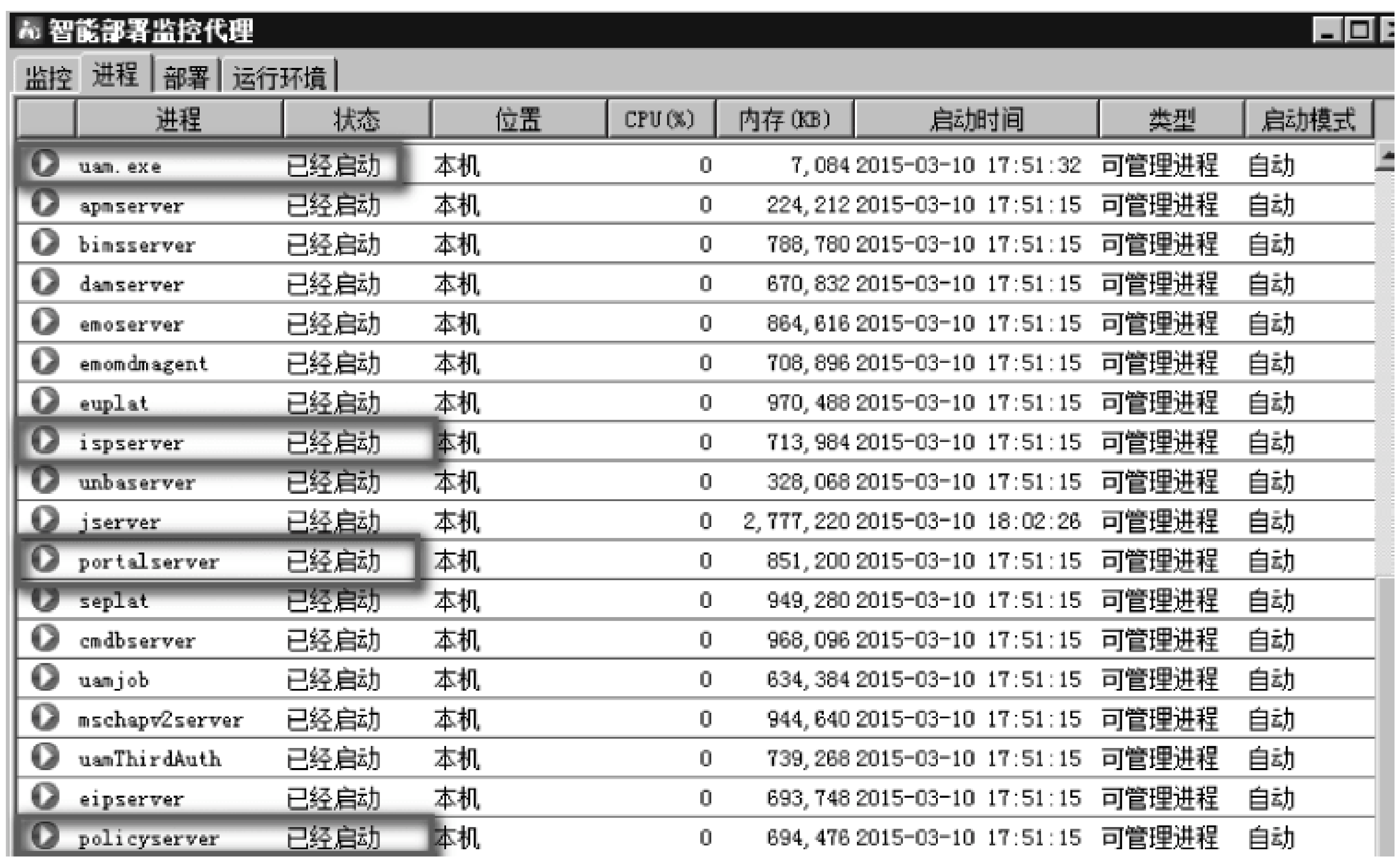


图 8-234　各进程启动情况

说明:

(a) 一般情况下,这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) portalserver 提供 Portal 认证功能。

(c) policyserver 主要用来提供客户端类功能。

(d) uam 进程提供用户认证功能。

(e) ispserver 统一代理服务器与 iNode 客户端的通信。

② 检查 iMC 服务器 1812、1813、9019、50100 和 50200 UDP 端口是否被上述相关进程监听,如图 8-235 所示。

说明:

(a) Windows 操作系统中,通过

netstat-aon | *findstr* :端口号

命令来显示某一端口的监听状态及其对应的进程 PID。



图 8-235　各端口被进程监听情况

(b) 1812、1813 所对应的进程 PID 应为 uam 相关的进程。

(c) 1812、1813 对应的 IP 应为 UAM 服务器实际 IP 地址。

(d) 9019 端口所对应进程 PID 为 ISP 相关进程，所对应的 IP 地址应为 0.0.0.0。

(e) 50100、50200 端口所对应进程 PID 为 Portal 相关进程，所对应的 IP 地址应为 0.0.0.0。

(f) Linux 系统命令

netstat-apn | grep：端口号。

③ 检查“iMC 智能监控代理”→“运行环境”选项卡，数据库连接状态是否正常，如图 8-236 所示。

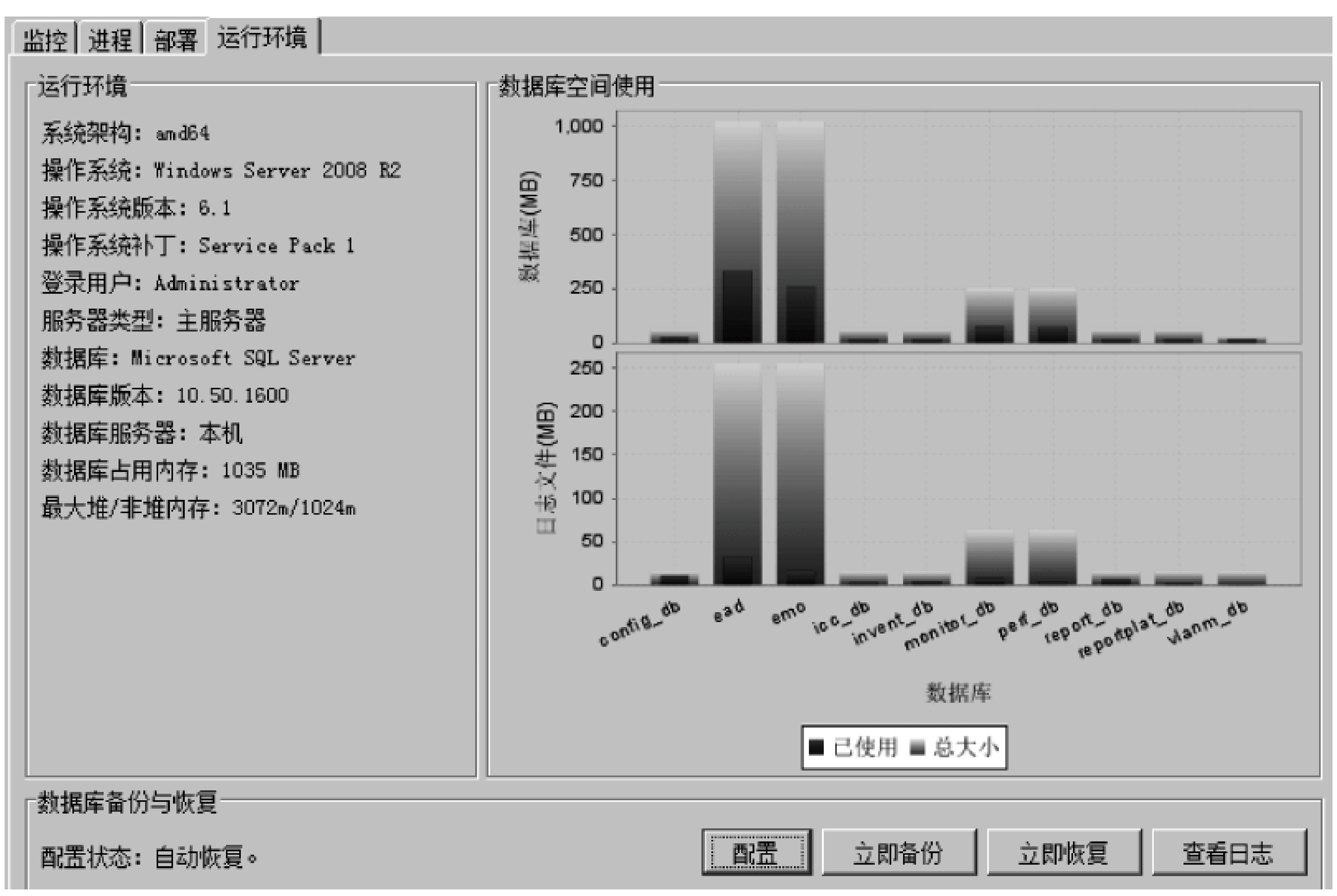


图 8-236　数据库连接状态

(3) 路由可达性检查

① 单击“用户”→“用户接入管理”→“接入设备管理”命令需添加接入设备发给 iMC 服务器 Radius 协议报文的端口 IP，iMC 默认会同该 IP 进行 Radius 协议报文交互，需保证 iMC 可以 ping 通该 IP，本例中接入设备 IP 应为 172.16.100.1。

② 对于 Portal 认证场景，需要保证认证前后认证客户端和 Portal 服务器路由可达，保证 Portal nas-ip 和 Portal 服务器路由可达，Portal nas-ip 默认为用户网关 172.16.16.1。

③ 保证 iNode 客户端认证通过后，终端可以与策略服务器正常通信。

说明：

(a) 接入设备会有多个 IP 地址，如果要更改接入设备 IP，需在 Radius Scheme 视图下配置如下命令，iMC 侧需同步修改：

[sw-radius-h3c]nas-ip 172.16.2.1，并在 iMC 上更改为 172.16.2.1。

(b) Portal 认证方式更改 Portal nas-ip 后需在 Interface-vlan 视图下配置命令，iMC 侧需同步修改：

[sw-vlan-interface6]portal nas-ip 192.168.6.1。

(c) iMC 通过策略服务器向 iNode 客户端下发防内网外连所需的 ACL，需要保证 iNode 到服务器 UDP 9019 端口可达。

(4) 适用条件检查

① 防内网外连功能需要与 802.1x 或 Portal 认证结合。

② 认证客户端必须为 iNode。

③ 客户端操作系统必须为 Windows。

④ 使用 3G 上网卡作为认证网卡时不支持防内网外连。

⑤ 通过 WAN 端口转发 IP 报文的 3G 上网卡只有作为非认证网卡时支持防内网外连。

说明：

(a) 对内网还是外网的判断依据是接入协议。如果 PC 使用的接入协议为 802.1x 或 Portal，则认为 PC 正在使用内网，否则认为 PC 访问外网，所以防内网外连功能必须与 802.1x 或 Portal 认证配合。

(b) 防内网外连功能仅对 IP 报文有效，对于红外、蓝牙等点对点设备无效，这种情况可以使用 DAM 的外设管理功能来禁用红外、蓝牙的设备。

(c) 通过其他私有方式转发 IP 报文的 3G 上网卡在 Windows Vista 及以上版本的操作系统中不支持防内网外连，XP 系统下，只有在 3G 网卡作为非认证网卡的应用场景下支持防内网外连。

(5) 设备配置检查

本文对认证相关的基本配置不做赘述，只是针对防内网外连功能所需特殊配置进行检查。防内网外连功能要求认证方案为扩展模式，相关命令如下。

```
[BAS-radius-h3c]display this
 radius scheme h3c
 server-type extended-------配置为扩展模式
 primary authentication 172.16.100.61
 primary accounting 172.16.100.61
 key authentication 123
 key accounting 123
 nas-ip 172.16.100.1
```

说明：

① 802.1x 认证模式为 EAP 或 Portal 端口组配置为 EAP 认证方式时可以配置标准模式 Radius Scheme。

② 接入设备配置的 key 值需与 iMC 侧接入设备配置的 key 值保持一致。

③ 与第三方接入设备配合认证时需保证该设备可以透传 EAP 认证报文。

（6）客户端 ACL 配置检查

iNode 客户端通过向 PC 网卡下发在线非认证网卡 ACL 和离线 ACL 实现防内网外连功能。单击“用户”→“安全策略管理”→“终端访问控制管理”→“客户端 ACL 管理”命令确认配置的客户端 ACL 是否存在问题，如图 8-237 所示。



图 8-237　确认配置的客户端 ACL 是否存在问题

单击“修改”按钮查看配置的具体 ACL 规则，如图 8-238 所示。



图 8-238　查看配置的具体 ACL 规则

说明：

① 在线非认证网卡 ACL：用户在线时所有非认证网卡应用的 ACL。

② 离线 ACL：用户下线后，所有网卡应用的 ACL。

③ iNode 客户端在线或离线时的受控规则如下。

用户上线前，所有网卡应用定制防内网外连功能时配置的默认规则，放行或丢弃所有报文，用户上线成功后，认证网卡访问网络不受限制；所有非认证网卡应用在线非认证网卡 ACL。如果未配置在线非认证网卡 ACL，则所有非认证网卡继续使用默认规则；用户下线

后，所有网卡应用离线 ACL 或 ping 情况离线 ACL。如果未配置离线 ACL 或 ping 情况 ACL，则所有网卡继续使用默认规则。

用户下线后，所有网卡应用离线 ping 监控服务器来监控内网外连。

④ 如果 iNode 客户端未定制防内网外连功能，而 iMC 的服务中启用了防内网外连，则客户端身份认证成功后随即下线，同时会显示 iMC 下发的提醒信息“服务器要求客户端启用防内网外连功能”。

(7) 内网外连策略检查

客户端 ACL 配置没有问题后需要确认内网外连策略是否应用了正确的客户端 ACL，点击“用户”→“安全策略管理”→“终端访问控制管理”→“内网外连策略”命令查看内网外连策略信息是否正确，是否引用了正确的客户端 ACL，如图 8-239 所示。

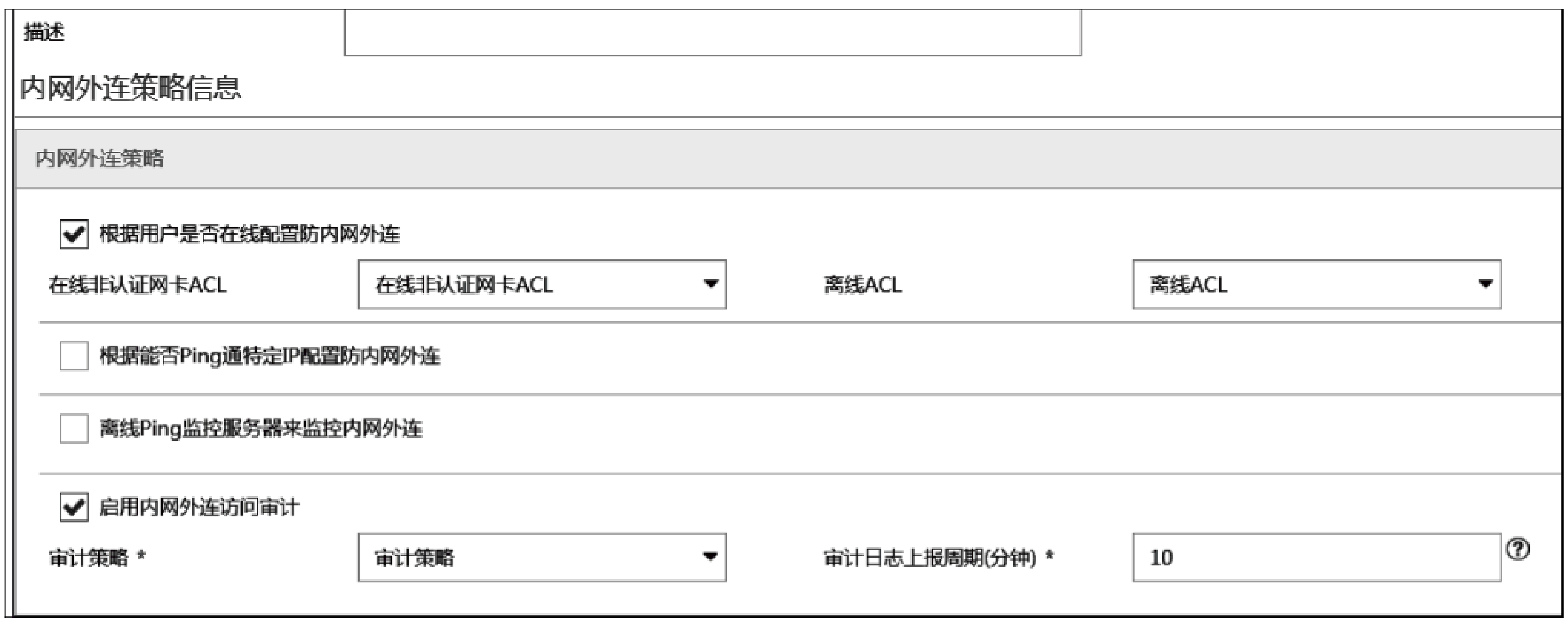


图 8-239 内网外连策略检查

说明：

① 根据用户是否在线配置防内网外连分为如下两种情况。

在线非认证网卡 ACL：用户在线时，非认证网卡应用的 ACL。下拉框中的 ACL 规则，在“用户”→“安全策略管理”→“终端访问控制管理”→“客户端 ACL 管理”中配置。

离线 ACL：当前用户下线后，所有网卡应用的 ACL。下拉框中的 ACL 规则，在“用户”→“安全策略管理”→“终端访问控制管理”→“客户端 ACL 管理”中配置。

② 根据能否 ping 通特定 IP 配置防内网外连：当前用户下线后，根据 ping 通特定 IP 的情况配置所有网卡的 ACL。如果下发了该配置，将优先应用于离线 ACL。

目的 IP 地址：离线 ping 特定 IP 的设置，最多设置两个，可以只配置一个。

ping 通离线 ACL：当前用户下线后，在 ping 通特定 IP 的情况下所有网卡应用的 ACL。

ping 不通离线 ACL：当前用户下线后 ping 不通特定 IP 情况下所有网卡应用的 ACL。

③ 离线 ping 监控服务器来监控内网外连：当前用户下线后，是否能 ping 通设置的“监控服务器 IP”来判断该机器是否连接了外网。

监控服务器 IP：设置的监控服务器的 IP 地址，可以设置多个。

最大记录数：防内网外连配置离线监控最大记录数，超出的将自动覆盖旧的记录。

ping 间隔：终端 ping 离线监控服务器的时间间隔。

④ 启用该项后 iNode 在离线的情况下会定时 ping 监控服务器，如果能 ping 通则进行记录并在 iNode 下次接入网络后上报给 iMC 服务器以供审计。

⑤ 内网外连审计：用户在线时，非认证网卡访问外网的结果审计。

⑥ 审计策略：下拉框中的审计策略，单击“用户”→“安全策略管理”→“终端访问控制管理”→“内网外连审计策略”命令中配置。

(8) 内网外连审计策略检查

单击“用户”→“安全策略管理”→“终端访问控制管理”→“内网外连审计策略”命令，配置需要进行审计的网段，如图 8-240 所示。



图 8-240　内网外连审计策略检查

说明：

① iNode 仅支持用户在线时非认证网卡访问外网的审计，不支持离线审计。

② 在防内网外连策略里面调用该审计策略。

(9) uam 服务配置检查

确认账号引用的服务配置了正确的防内网外连策略，如图 8-241 所示。



图 8-241　uam 服务配置检查

说明：

① 服务后缀需要与设备侧配置的域名保持一致，可以为空，具体请参考云图《iMC 802.1x 认证问题排查指导》。

② V5 版本 iMC 必须使用安全策略才可以启用防内网外连功能，V7 版本不再依赖 EAD 安全策略。

(10) uam 账号配置检查

检查账号是否申请了对应的接入服务，如图 8-242 所示。



图 8-242　uam 账号配置检查

说明：

① 检查账号状态是否正常，是否在有效期内。

② 检查接入服务配置。

(11) iNode 客户端配置检查

确认 iNode 客户端订制了防内网外连功能。确认方法如下：打开管理中心，单击“历史定制信息”命令，找到定制发生时间后，单击“详细信息”命令，就会出现如图 8-243 所示。

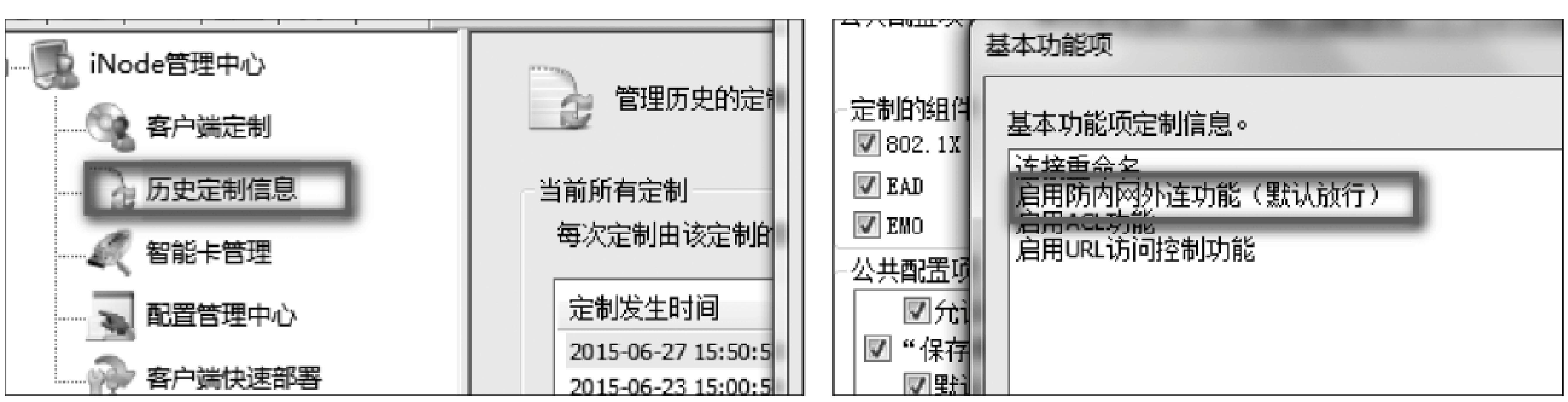


图 8-243　确认 iNode 客户端订制了防内网外连功能

同时确认 iNode 侧驱动安装正常，驱动安装正常时在“网络连接”→“属性”里面显示如图 8-244 所示，如果安装不正常可以通过重装或修复 iNode 解决。

说明：

① 订制客户端时需要从基本功能项里面勾选“防内网外连”并选择默认动作。

② 客户端防内网外连功能通过安装一个 NDIS Intermediate 过滤驱动来实现。此驱动随 iNode 客户端安装卸载。驱动安装完成后，将被 Windows 自动加载到每一个网卡中。每一个



图 8-244　确认 iNode 侧驱动安装正常

经过网卡的报文均会经过此驱动，因此报文会被过滤。驱动的启动和停止依赖于网卡的启停，而不依赖于 iNode。因此无论 iNode 是否启动，驱动都会对流出方向的 IP 报文进行过滤。

③ 由于驱动位于系统 IP 协议栈之下，所以无论网络接口是什么形态(包括以太网卡、Modem、GPRS/CDMA 移动上网卡等)，只要是以 IP 包传输数据，均可以过滤。

④ iNode 客户端成功完成 802.1x 或 Portal 认证后，iNode 会给完成认证网卡的驱动实例下发指令解除过滤，从而使认证网卡不受限制。当用户下线后，iNode 会再次下发指令恢复过滤。

⑤ 认证终端如果安装有多个带有驱动功能的软件时，建议最先安装 iNode。

(12) 用户日志审计

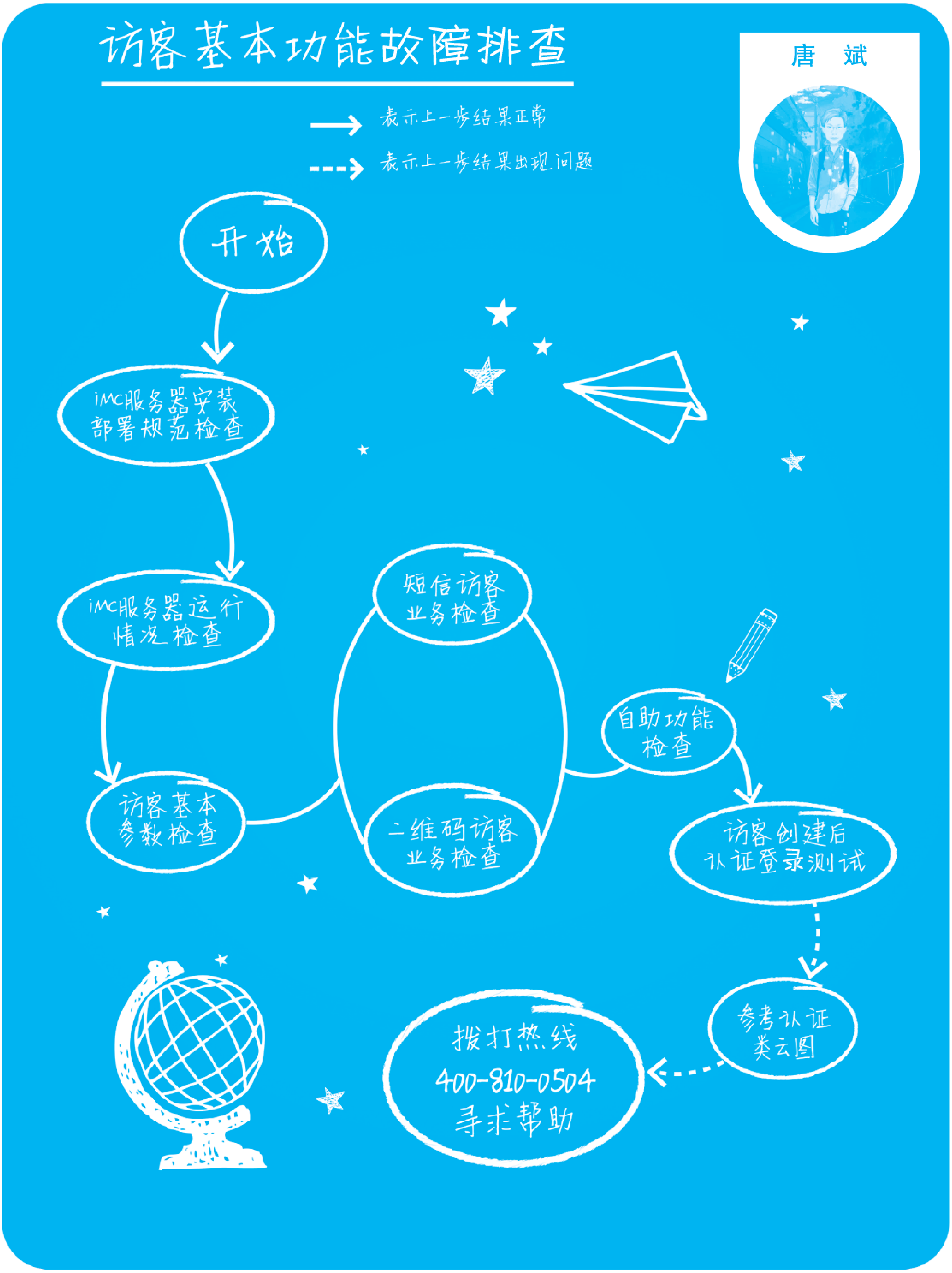
单击“用户”→“用户接入日志”→“内网外连访问审计日志”命令，里面可以查询到用户在线时非认证网卡访问外网的情况，如图 8-245 所示。

在线内网外连访问审计日志列表

帐号名 ⇕	用户姓名 ⇕	开始时间(服务器)	结束时间(服务器)	目的IP地址 ⇕	目的端口号 ⇕	协议号 ⇕	报文个数 ⇕	详细信!
802	802	2015-06-27 16:53:09	2015-06-27 16:55:46	10.72.66.37	53	17	130	
802	802	2015-06-27 16:53:09	2015-06-27 16:55:46	10.153.0.68	53	17	126	
802	802	2015-06-27 16:53:09	2015-06-27 16:55:46	10.72.66.36	53	17	106	

图 8-245　用户日志审计

说明：审计日志上报间隔由防内网外连策略里面配置的审计上报周期决定，不足一个周期的由 iNode 下次上线时上报。


访客基本功能故障排查
唐 斌
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
访客基本参数检查
短信访客业务检查
二维码访客业务检查
自助功能检查
访客创建后认证登录测试
参考认证类云图
拨打热线
400-810-0504
寻求帮助

1. 开始

访客管理系统适用于需要频繁接待外来人员的企业或公司。主要使用场景有以下两种。

(1) 接待零散访客：将接待人员使用的 iMC EIA 接入用户指定为访客管理员，由访客管理员直接登录用户自助服务平台中直接创建访客。访客创建后即生效。

(2) 集体访客(如公司组织的大型培训等)：由访客自行登录用户自助服务平台中预注册访客，预注册时指定访客管理员。然后由对应的访客管理员登录到用户自助服务平台中激活访客。访客激活后即生效。

应用方式主要有 3 种：①访客预注册＋访客管理员转正审批的流程。②访客预注册＋免审批、自动转正的流程。③访客管理员直接为来访人员创建访客账号的流程。

访客基本功能的排错思路：访客功能基于基本的认证环境，须确保基本认证没有问题。关于认证故障的排查请查阅认证类云图。访客排错首先检查服务器软硬件运行状态，主要关注访客功能对应组件的部署情况、进程运行状态。然后对访客业务基本参数进行检查。再之后对访客的策略配置、服务配置、管理员配置相应的进行检查。最后若访客创建没有问题，可以手动创建访客后，测试其他功能。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“用户接入管理”→“用户自助服务”是已部署的状态。若访客应用涉及终端识别，则“用户接入管理”→“EIP 服务器”组件也应处于部署状态。具体如图 8-246 所示，关于其他“用户接入管理”组件的检查方式，请参考认证类云图。

(2) iMC 服务器运行情况检查

要使用访客功能，除了确保 UAM 相关进程运行正常外，还要检查 JServer 是否正常，可使用以下方法简单查看。

① 单击“开始”→“智能部署监控代理”命令，选择“进程”标签，检查访客功能主要进程为 jserver 进程，若分布式部署时检查进程 webserver。其他“用户接入管理”进程请参考认证类云图。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

组件名	描述	版本	状态	部署位置
智能策略服务代理	提供统一的策略服务代理功能...	iMC ISP 7.1 (E0305)	已部署	主服务器
用户接入管理 - 用户接入管理	提供对接入用户、接入业务的...	iMC UAM 7.1 (E0305)	已部署	主服务器
用户接入管理 - Portal服务器	提供Portal认证功能。	iMC UAM 7.1 (E0305)	已部署	主服务器
用户接入管理 - EIP服务器	提供终端智能识别的功能。	iMC EIP 7.1 (E0305)	已部署	主服务器
用户接入管理 - EIP从服务器	部署在EIP服务器之外的其他...	iMC EIP 7.1 (E0305)	未部署	
用户接入管理 - 策略服务器	提供安全认证的功能。	iMC UAM 7.1 (E0305)	已部署	主服务器
用户接入管理 - 用户自助服务	提供用户资料的自助查询和维...	iMC UAM 7.1 (E0305)	已部署	主服务器
用户接入管理 - 用户接入管理从服务器	部署在用户接入管理服务器之...	iMC UAM 7.1 (E0302)	未部署	
自主页面定制Web服务器	提供一个独立的Web容器，用...	iMC UAM 7.1 (E0305)	已部署	主服务器
用户接入管理 - Portal服务器	提供Portal认证功能。	iMC UAM 7.1 (E0305)	未部署	
自主页面定制Web服务器	提供一个独立的Web容器，用	iMC UAM 7.1 (E0305)	未部署	

图 8-246　部署状态

② iMC 服务运行情况检查具体如图 8-247 所示。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
imcvlandm.exe	已经启动	本机	0	17,076	2015-07-22 13:57:49	可管理进程	自动
img.exe	已经启动	本机	0	7,544	2015-07-22 13:57:44	核心进程	自动
tam.exe	已经启动	本机	0	15,636	2015-07-22 13:57:49	可管理进程	自动
tftpserver.exe	已经启动	本机	0	9,116	2015-07-22 13:57:33	可管理进程	自动
uam.exe	已经启动	本机	0	27,076	2015-07-26 03:00:03	可管理进程	自动
uamimg.exe	已经启动	本机	0	7,744	2015-07-22 13:57:51	核心进程	自动
apmserver	已经启动	本机	0	222,132	2015-07-22 13:57:22	可管理进程	自动
damserver	已经启动	本机	0	204,344	2015-07-22 13:57:24	可管理进程	自动
emoserver	已经启动	本机	0	252,628	2015-07-22 13:57:24	可管理进程	自动
emomdmagent	已经启动	本机	0	366,496	2015-07-22 13:57:24	可管理进程	自动
ispserver	已经启动	本机	0	213,404	2015-07-22 13:57:24	可管理进程	自动
jserver	已经启动	本机	0	1,293,292	2015-07-22 13:57:24	可管理进程	自动
portalserver	已经启动	本机	0.04	245,036	2015-07-22 13:57:24	可管理进程	自动
uamjob	已经启动	本机	0.04	396,256	2015-07-22 13:57:24	可管理进程	自动
uamThirdAuth	已经启动	本机	0	315,052	2015-07-22 13:57:24	可管理进程	自动
mschapv2server	已经启动	本机	0	255,456	2015-07-22 13:57:24	可管理进程	自动
eipserver	已经启动	本机	0	249,548	2015-07-22 13:57:24	可管理进程	自动
policyserver	已经启动	本机	0	221,700	2015-07-22 13:57:24	可管理进程	自动
difserver	已经启动	本机	0	215,440	2015-07-22 13:57:24	可管理进程	自动
stmserver	已经启动	本机	0	230,248	2015-07-22 13:57:24	可管理进程	自动
acmweb	已经启动	本机	0	249,096	2015-07-22 13:57:24	可管理进程	自动

图 8-247　iMC 服务运行情况检查

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) 通过 netstat -aon|findstr ：端口(通常为 80 或 8080)，查看查询结果中 PID 是否 java 进程对应的 PID 一致。

(c) 若“用户接入管理”→“用户自助管理”组件分布式部署其他服务器，则从机上查看的进程为 webserver 进程。同时主服务查看 jserver 进程。

(3) 访客基本参数检查

① 访客业务参数配置。

系统参数是访客相关的常用参数，可以根据实际需求进行修改，如图8-248所示。



图8-248 访客业务参数配置

说明：

(a) 失效访客保留时长：访客对应的账号失效后，账号在系统中保存的时长。超时后访客将被自动删除。

(b) 默认访客用户分组：该参数决定了访客管理员在自助系统中增加的访客，以及在自助系统中激活的预注册访客所属的用户分组。

(c) 短信开户获取密码间隔时长：访客注册简化页面进行短信开户时，如果开户成功，再次获取密码需要等待的时长。

(d) 访客预注册：该参数控制是否启用访客预注册功能，超过15天未正式注册的预注册访客会被系统自动清除。

(e) 允许同一电话被多个访客使用：该参数控制访客注册和预注册时，是否允许同一电话被多个访客使用。

(f) 预注册访客关联已存在的用户：选择禁止表示在预注册访客时，如果访客姓名与证件号码已经存在，则注册失败。选择允许则可以关联到已存在的用户。

② 访客管理员配置。

访客管理员的主要功能是管理访客和激活预注册访客。访客管理员和访客的关联关系在增加访客或预注册访客时确立。

访客管理员分为两种类型：访客管理员和超级访客管理员。访客管理员只能管理名下的访客和预注册访客。超级访客管理员可以管理所有的访客和预注册访客。

若希望访客转正模式是自动转正，则必须设置默认访客管理员。如图8-249所示，标红处设置默认访客管理员。

已经增加为访客管理员的用户分组，如果增加的接入用户关联了此用户分组，那么增加的接入用户默认为访客管理员。如图8-250所示用户分组imc，其中的接入用户都关联为访客管理员。



图 8-249　设置默认访客管理员



图 8-250　关联访客管理员

说明：单击默认访客管理员列中的链接，可以为在 Portal 页面自动注册的访客指定管理员。注意，只能将一个访客管理员设置为默认访客管理员。

③ 访客服务配置。

访客服务是专门供访客接入网络的服务，在功能上与接入用户使用的服务基本一致，如图 8-251 所示。



图 8-251　访客服务配置

说明：

(a) 分配 IP 地址的服务不能设置为访客服务。

(b) 访客使用的访客服务即使使用了计费策略也不会计费。访客服务使用计费策略主要是为了达到限制访客用户接入网络时长的目的。

(c) 单击默认访客服务列中的链接，设置该服务是否为默认的访客服务。该功能用于无法选择访客服务的场景：短信开户与认证、二维码开户与认证的自动转正方式、自助服务访客

预注册的自动转正方式、BYOD 访客预注册的自动转正方式、智能终端访客管理员自助平台中的访客审批、访客注册。注意，只有一个服务可以用于访客的自动转正。

④ 访客策略配置。

访客策略用于增加访客和预注册访客的相关参数配置，其中具体包括基本信息、访客参数、访客服务和访客用户分组的配置。未配置访客策略的访客用户分组则使用默认访客策略，如图 8-252 所示。

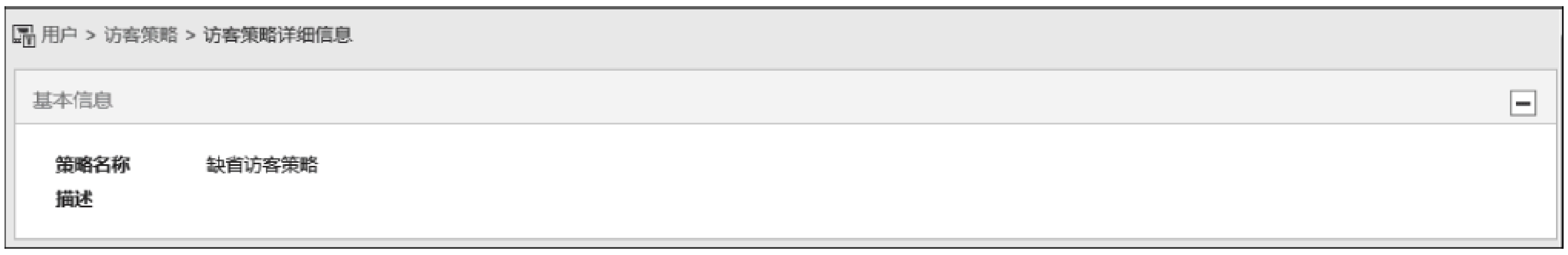


图 8-252　默认访客策略

(a) 基本功能。图 8-253 所示为基本功能。



图 8-253　基本功能

说明：

ⓐ 预注册访客自动转正：如果选择"允许"表示终端用户预注册为访客后自动转正，而不需要访客管理员审批转正。如果选择"禁止"表示需要访客管理员审批后，预注册访客才能转正。只有当单击"访客管理"→"访客业务参数配置"命令中的"访客预注册"设置为"允许"时，该参数才生效。允许访客自动转正时，必须指定默认访客管理员和默认访客服务。

ⓑ 访客密码通知方式：选择告知访客登录密码等信息的方式。告知方式包括短信和电子邮件，可以同时选择两种方式。如果告知方式为短信，则需要启用短信功能，详细说明请参见短信功能配置；短信的内容在"消息下发"中定制。如果告知方式为电子邮件，邮件的内容由 UAM 预置，无法修改；同时只有在 iMC PLAT 中配置正确的邮件服务器，才能成功发送邮件。如果未选择任何一种方式，表示不将密码通知到访客。

ⓒ 访客预注册后显示二维码：访客预注册以及预注册自动转正(除 BYOD 方式)的结果页面是否显二维码。

ⓓ 访客在线数量限制默认值：输入访客注册页面中"在线数量限制"默认显示的值。

ⓔ 访客在线数量限制最大值：输入访客注册页面中"在线数量限制"可以配置的最大值。

ⓕ 访客生效方式：如果选择"手工指定生效时间"表示访客管理员可以手工指定所管理访客的生效时间和失效时间，如果选择"首次上线生效"表示访客首次上线后更新生效时间和失效时间。除了移动访客管理自助平台注册的访客，其他方式注册的访客转正时，访客生效时间都受该参数控制。

(b) 访客用户默认值和快捷开户。图 8-254 所示为访客用户默认值和快捷开户。



图 8-254　访客用户默认值和快捷开户

说明：访客用户的默认值设置如下。

ⓐ Portal 无感知认证最大绑定数：如果选择 1～5 表示使用该账号进行 Portal 无感知认证的终端数不能超过所选的值。如果选择“不支持绑定”表示不能使用该账号进行 Portal 无感知认证。只有当“访客管理”→“访客业务参数配置”中的“访客预注册”设置为“允许”时，该参数才生效。

ⓑ 默认访客有效时长：输入默认情况下，访客的有效时长。注册访客时，如果未设置或无法设置失效时间，则访客的失效时间取该参数和“所管理访客的最大有效时长”的较小值。“所管理访客的最大有效时长”在增加访客管理员时配置，具体请参见增加访客管理员。

ⓒ 访客密码有效时长：输入访客密码的有效时长，从访客生效时开始计算。访客只在密码失效前才能接入网络。如果该参数保持为空，则表示访客密码永不失效。

ⓓ 访客密码生成规则：系统自动生成访客密码的规则。UAM 支持三种规则，即 n 位数字、n 位字母和 n 位数字＋字母的组合。该规则对访客注册过程中手工输入的密码无效。

快捷开户方式如下。

ⓔ 短信开户与认证页面的校验方式：如果选择“指定授权码方式”，则还需配置授权码。如果选择“随机验证码方式”后，在“短信开户与认证页面”会显示含有随机信息的图片，只有正确输入了图片中的内容才能进行注册；如果选择“指定授权码方式”后，在“短信开户与认证页面”中会要求终端用户输入授权码，只有正确输入授权码才能进行访客注册。如果选择“不验证”后，终端用户直接可以进行访客注册。“随机验证码方式”和“指定授权码方式”可以防止恶意注册。

ⓕ 访客账号名生成规则：如果选择“前缀＋系统时间的毫秒值”，则还需配置前缀。例如：假设某个访客在 2014 年 1 月 1 日 8 点 8 分 8 秒 123 毫秒开户（该时间对应的毫秒值为 1388534888123），如果选择“系统时间的毫秒值”，则账号名为 1388534888123；如果选择“前缀＋系统时间的毫秒值”，且“前缀”配置为“auto”，则账号名为 auto1388534888123；如果选择“YYMMDDhhmmss 时间戳＋4 位随机数”，则账号名为 140101080808ZZZZ，其中 ZZZZ 是四位随机数字。

(c) 对于非默认的访客策略，可以选择使用的访客服务和策略生效的访客用户分组，如图 8-255 所示。



图 8-255 非默认的访客策略

说明：

ⓐ 一个访客策略可以配置多个访客用户分组，一个访客用户分组只能被一个策略使用。

ⓑ 触屏版用户自助平台不支持自定义的访客策略。

ⓒ 直接在访客用户分组列表中选择访客策略关联的分组。无法选择已经关联了其他访客策略的分组。

ⓓ 选项"选择用户分组时自动选中其父分组和子分组"。如果选中该项，每选择一个分组，UAM 都会自动选择该分组的父分组和子分组。取消选择亦是如此。

(d) 短信访客业务检查。

如果要使用短信访客自动开户的功能，必须满足以下所有条件。

ⓐ 配置短信发送功能

iMC Plat 7.1E0303P13 之后，iMC 上配置短信功能界面统一在"系统管理"下。该功能用于配置短信发送功能的参数。"其他厂商短信平台"是指用户自定义的第三方短信平台，需要进行二次开发。具体短信猫设置和短信平台配置请参考配置手册。"邮箱转短信"本文档不涉及，如图 8-256 所示。



图 8-256 短信发送功能

说明：

（Ⅰ）使用短信猫作为发送方式效率很低，一分钟只能发送四条信息，可能会出现用户无法接收短信的现象。对于批量发送短信的功能，建议使用短信平台来操作。

（Ⅱ）使用短信平台作为发送方式时，若注册序列号失败，并且返回错误码为-1100，则需要手动修改文件 iMC 安装目录\client\repository\imc\jars\emay.jar 中的 config.properties 文件内容，然后重启 iMC。因注册码的格式不同，修改的 config.properties 文件内容不同。

序列号格式与 config.properties 文件内容对应如下。

3SDK-EMY-0130-XXXXX

url=http://sdkhttp.eucp.b2m.cn/sdk/SDKService?wsdl

9SDK-EMY-0999-XXXXX

url=http://sdk999ws.eucp.b2m.cn:8080/sdk/SDKService?wsdl

6SDK-EMY-6688-XXXXX

url=http://sdk4report.eucp.b2m.cn:8080/sdk/SDKService?wsdl

9SDK-EMY-0229-XXXXX

url=http://sdk229ws.eucp.b2m.cn:8080/sdk/SDKService?wsdl

如果仍存在问题，请联系序列号提供商。

ⓑ 进行短信功能配置。

选择读取用户手机号码信息的方式，如图 8-257 所示。



图 8-257　短信功能配置

说明：手机号码获取方式：系统提供了如下 3 种获取发送手机号码的方式。

（Ⅰ）电话号码：获取用户注册时填写的电话号码，作为发送短信的号码。

（Ⅱ）账号名：获取用户的账号名，如果账号名符合电话号码规范，作为发送短信的号码。

（Ⅲ）电话号码与账号名：优先取用平台用户的“电话”为短信号码，平台用户电话的限制为：数字、“(”“)”“+”“-”和空格，取用时将保持原值，不会处理其中的特殊字符。如果平台用户没有“电话”，则再尝试取值 UAM 接入账号名，有平台用户电话一样的限制：数字、“(”“)”“+”“-”和空格。若平台用户无电话，接入账号名也不符合要求，则不发短信。

ⓒ 配置短信内容。

在用户短信通知内容配置，定制密码通知的短信内容，如图 8-258 所示。

说明：

（Ⅰ）系统基于用户分组查找对应的短信内容，如果没有找到指定的记录，则不会发送短信。

（Ⅱ）一个用户分组只能被一个用户短信通知使用。

说明：简单测试短信功能正常的方法如下。

选择或建立一个有手机号码信息的测试用户，在接入用户详细信息界面的右侧“动作”栏中，单击“密码通知短信”。若成功，则右上角提示发送短信成功，若失败，则根据错误提示排查



图 8-258　短信内容配置

或拨打华三 400 寻求技术支持，如图 8-259 所示。



图 8-259　简单测试短信功能方法

ⓓ 配置访客预注册和自动转正功能。

启用访客系统参数：访客预注册。启用访客策略参数：预注册访客自动转正。请参考本文档第(3)步，此处不赘述。

ⓔ Portal 端口组下选用短信开户与认知页面。

根据 Portal 端口组信息配置中的页面推送策略不同，配置有所不同。如果不选用页面推送策略，则默认认证页面选择短信开户与认证。如果选用页面推送策略，则需要在页面推送策略中将短信开户与认证页面增加为使用特定场景的用户所使用的页面，如图 8-260 所示。

说明：

(Ⅰ) 页面推送策略：根据配置的页面推送策略，在页面推送策略配置中找到对应的认证页面，用户访问 Portal 服务器将被重定向到此页面。如果所配置的页面推送策略为空或没有



图 8-260　页面推送策略

找到配置的认证页面，用户访问 Portal 服务器将被重定向到配置的默认认证页面。具体配置及使用方法请登录 kms.h3c.com 查找。

（Ⅱ）默认认证页面：Portal 用户认证的页面，列表中罗列了系统预定义的页面和“用户”→“接入策略管理”→“终端页面定制”→“Portal 页面定制”中为 PC 和手机定制的 Portal 页面。系统预定义的页面包含默认“短信开户与认证(PC、Phone)”页面。

(e) 二维码访客业务检查

ⓐ 如果是 Portal 场景，必须满足以下所有条件。

启用访客系统参数：访客预注册。

请参考本文档第(3)步“访客基本参数检查”，此处不赘述。

配置 Portal 认证界面为二维码开户与认证页面。

根据 Portal 端口组信息配置中的页面推送策略不同，配置有所不同。如果不选用页面推送策略，则默认认证页面选择二维码开户与认证页面即可；如果选用页面推送策略，则需要在页面推送策略中将二维码开户与认证页面增加为使用特定场景的认证页面。

说明：

（Ⅰ）页面推送策略：略。

（Ⅱ）默认认证页面：Portal 用户认证的页面，列表中罗列了系统预定义的页面和“用户”→“接入策略管理”→“终端页面定制”→“Portal 页面定制”中为 PC 和手机定制的 Portal 页面。系统预定义的页面包含默认“二维码开户与认证(PC、Phone)”页面。

ⓑ 如果是 BYOD 场景，必须满足以下所有条件。

需要部署自助服务组件、EIP 组件。

请参考本文档第(1)步“iMC 服务器安装部署规范检查”。

启用如下访客系统参数：访客预注册

请参考本文档第(3)步“访客基本参数检查”。

存在默认访客管理员、默认访客服务。

请参考本文档第(3)步“访客基本参数检查”。

配置 BYOD 界面为二维码开户与认证页面。页面推送策略里选择认证方式为“MAC”，二维码开户与认证页面作为默认 BYOD 页面，如图 8-261 所示。

说明：

（Ⅰ）页面推送策略是为了用户通过不同的认证方式进行认证时，根据不同条件推送不同认证页面而配置的策略。

（Ⅱ）当用户访问 BYOD 页面时，根据 MAC 认证方式推送符合条件的认证页面。



图 8-261　配置 BYOD 界面为二维码开户与认证页面

① 配置了“页面推送策略”：则用户与认证页面的对应关系由“页面推送策略”功能的具体配置决定。如果在页面推送策略配置中没有找到匹配的认证页面，认证页面将使用页面推送策略默认 MAC 认证页面。

Ⅱ 未配置“页面推送策略”，BYOD 将推送默认 MAC 认证页面。

（Ⅲ）MAC 认证方式页面推送策略只能有一个。

（f）自助功能检查

检查系统参数自助组件端口配置。

访客功能依赖单击“接入用户管理”→“用户自助组件”命令，若需保证可以正常访问用户自助页面，如图 8-262 所示。



图 8-262　用户自助页面

配置界面单击“用户”→“接入策略管理”→“业务参数配置”→“系统配置”→“系统参数配置”命令下，自助页面的端口要与访问“http://IP:端口/selfervice”中的端口一致，如图 8-263 所示。

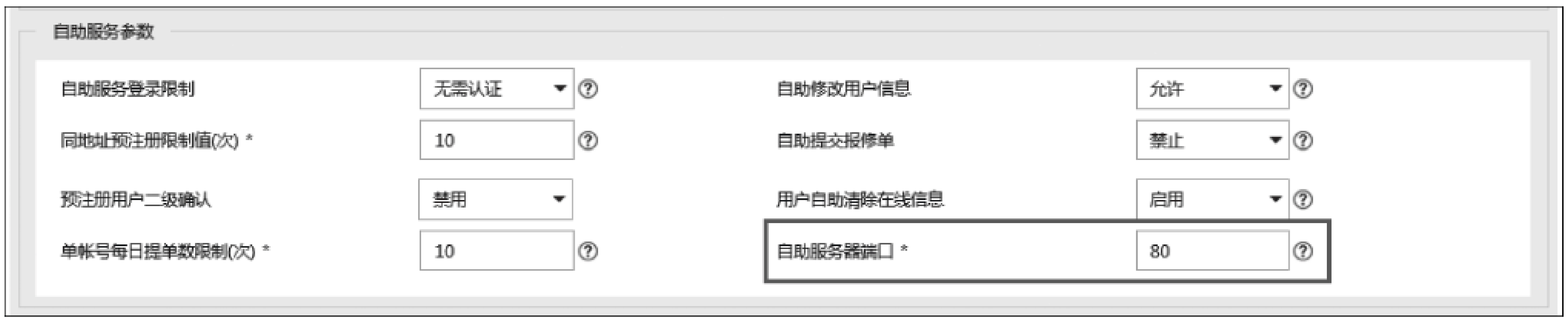


图 8-263　自助服务参数

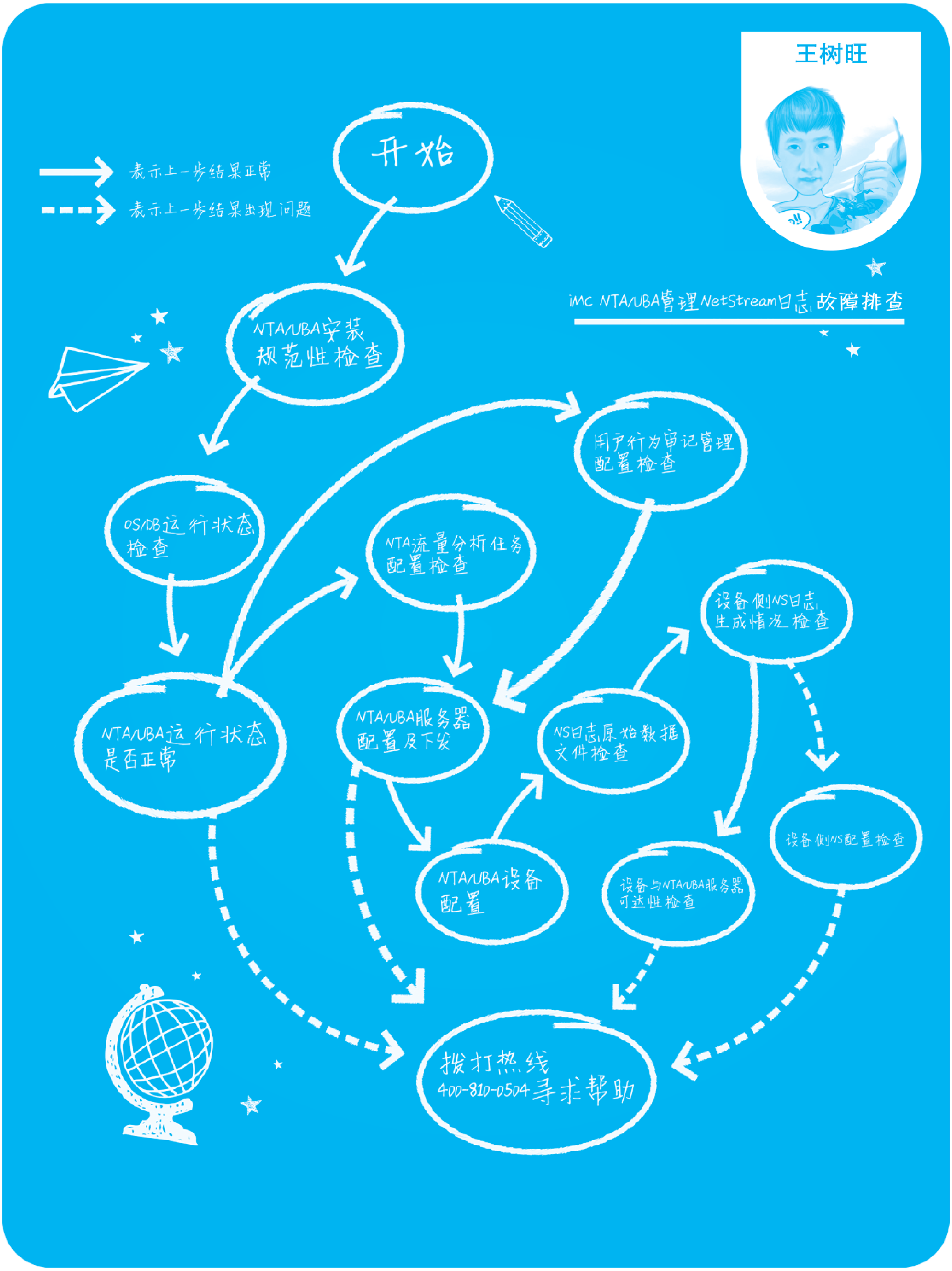
说明：自助服务器端口：只有出现以下情况时才需要修改。如果管理员修改了自助配置文件(＜iMC 安装目录＞\client\conf\http. properties)中的 imc. http. port，则必须将该参数也进行同步修改。例如，imc. http. port 由 8080 修改为 8088，则该参数也必须修改为 8088。修改完成在 iMC 部署监控代理中重启 JServer 进程，使自助配置文件的修改生效。如果 iMC 为分布式环境且自助服务组件部署在从服务器上，则只需重启自助服务组件所在从服务器上的 WebServer 进程即可。

(g) 访客创建后认证登录测试

查看所有访客界面，访客账号创建正常，基本信息正常。那么之后的认证类似于普通正常用户进行 Portal 或 802. 1x 认证，如图 8-264 所示。此时故障排查请参考认证类云图，或咨询 400 售后热线。



图 8-264　访客创建后认证登录测试


王树旺
iMC NTA/UBA管理NetStream日志故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
NTA/UBA安装规范性检查
OS/DB运行状态检查
NTA/UBA运行状态是否正常
用户行为审计管理配置检查
NTA流量分析任务配置检查
NTA/UBA服务器配置及下发
NTA/UBA设备配置
NS日志原始数据文件检查
设备侧NS日志生成情况检查
设备侧NS配置检查
设备与NTA/UBA服务器可达性检查
拨打热线
400-810-0504寻求帮助

1. 开始

iMC NTA/UBA 两个组件均有管理 NetStream 日志的功能，其中 NTA 面向网络流量分析，UBA 面向用户行为审计。iMC NTA/UBA 管理 NetStream 的问题排查思路主要分为以下两大部分。

① 设备侧是否将对应流量转换生成 NetStream 日志并将日志发送给 iMC NTA/UBA 服务器。

② iMCNTA/UBA 服务器是否收到设备侧的 NetStream 日志，是否能够缓存在本地然后写入数据库并最终展示出来。

2. 流程图相关操作说明

（1）NTA/UBA 安装规范性检查

对照《智能管理中心（iMC）部署和硬件配置方案》对现场 NTA/UBA 服务器的安装规范进行检查，排查现场的服务器硬件条件是否符合 NTA/UBA 服务器的安装规范要求。重点检查如下几点。

① NTA/UBA 服务器是否专机专用，即除了安装 iMC 之外不能安装其他类似的网络管理产品。

② 服务器的硬件配置符合 NTA/UBA 的安装及运行要求，重点关注服务器的磁盘性能、空间的情况。

③ 在大规模应用场景中，NTA/UBA 服务器是否进行了合理的分布式部署。

（2）OS/DB 运行状态检查

NTA/UBA 作为软件产品其运行依赖于底层操作系统及数据库的正常运行，这部分重点排查的内容有如下。

① 操作系统、数据库是否为正版软件。

② 操作系统、数据库是否已打上所需的补丁（对照 iMC PLAT/NTA/UBA 的版本说明书）。

③ 操作系统的系统时间配置是否正确。

（3）NTA/UBA 运行状态检查

这部分重点排查的内容如下。

① iMC 部署监控代理中各进程运行正常，无异常的进程。

② iMC NTA/UBA 服务器的 CPU、内存利用率正常。

（4）NTA 流量分析任务配置

NTA 的流量分析任务分为接口、VLAN、采集器、应用、主机、VPN、业务间 7 种，请注意 NetStream 日志情况下 NTA 不能进行采集器流量分析。

在单击“配置管理”→“流量分析任务管理”命令后可以查看到这些流量分析任务并可以单击进行详细页面检查对应的配置是否正确。

（5）用户行为审计管理配置

用户行为审计分为通用审计、地址转换审计、Web 访问审计、文件传输审计、邮件审计几

种，请注意 NetStream 日志情况下 UBA 仅能进行通用审计。

用户行为审计可以在“配置管理”→“用户行为审计管理”中进行查看并检查对应的配置是否正确。

(6) NTA/UBA 服务器配置

在单击“业务”→“配置管理”→“服务器管理”→“服务器配置”命令可以查看对应的服务器配置是否正确。

在服务器管理中可以单击“配置下发”按钮测试服务器配置能否正常下发到 NTA/UBA 接收器进程上，正常情况下会显示下发成功，如图 8-265 所示。



图 8-265 NTA/UBA 服务器配置

(7) NTA/UBA 设备配置

可以在单击 iMC NTA/UBA“业务”→“配置管理”→“设备管理”→“修改设备”命令后检查设备配置，请注意 SNMP 团体字对应设备上配置的 SNMP 读团体字，如图 8-266 所示。



图 8-266 NTA/UBA 设备配置

(8) NTA/UBA NetStream 原始日志数据文件检查

NTA/UBA 会将收到的 NetStream 日志先缓存到本地形成文件再逐一入库，该原始日志数据文件的保存路径为 NTA/UBA 部署所在服务器安装目录的 data/processorData/data 目录，正常情况下该目录应该有待入数据库的少量原始日志文件。如果没有说明情况异常，多为配置类问题；如果有大量的日志文件也是异常的，说明原始日志文件入数据库时存在积压的情况，需要排查数据库性能、磁盘空间是否足够等方面的因素，如图 8-267 所示。

(9) 设备侧 NetStream 日志生成情况检查

检测设备侧是否成功地将 NetStream 日志发送给 iMC NTA/UBA 服务器，重点关注发



图 8-267　NetStream 原始日志数据文件检查

送的目的 IP 地址、端口是否正确，是否有日志报文发送出来。

命令：*display ip netstream export*

如下中的 172.8.99.176 应该为 NTA/UBA 服务器的 IP 地址，对应的监听端口为 9020，同时已经成功的发送了 3292 个 NetStream V5 版本的日志报文。

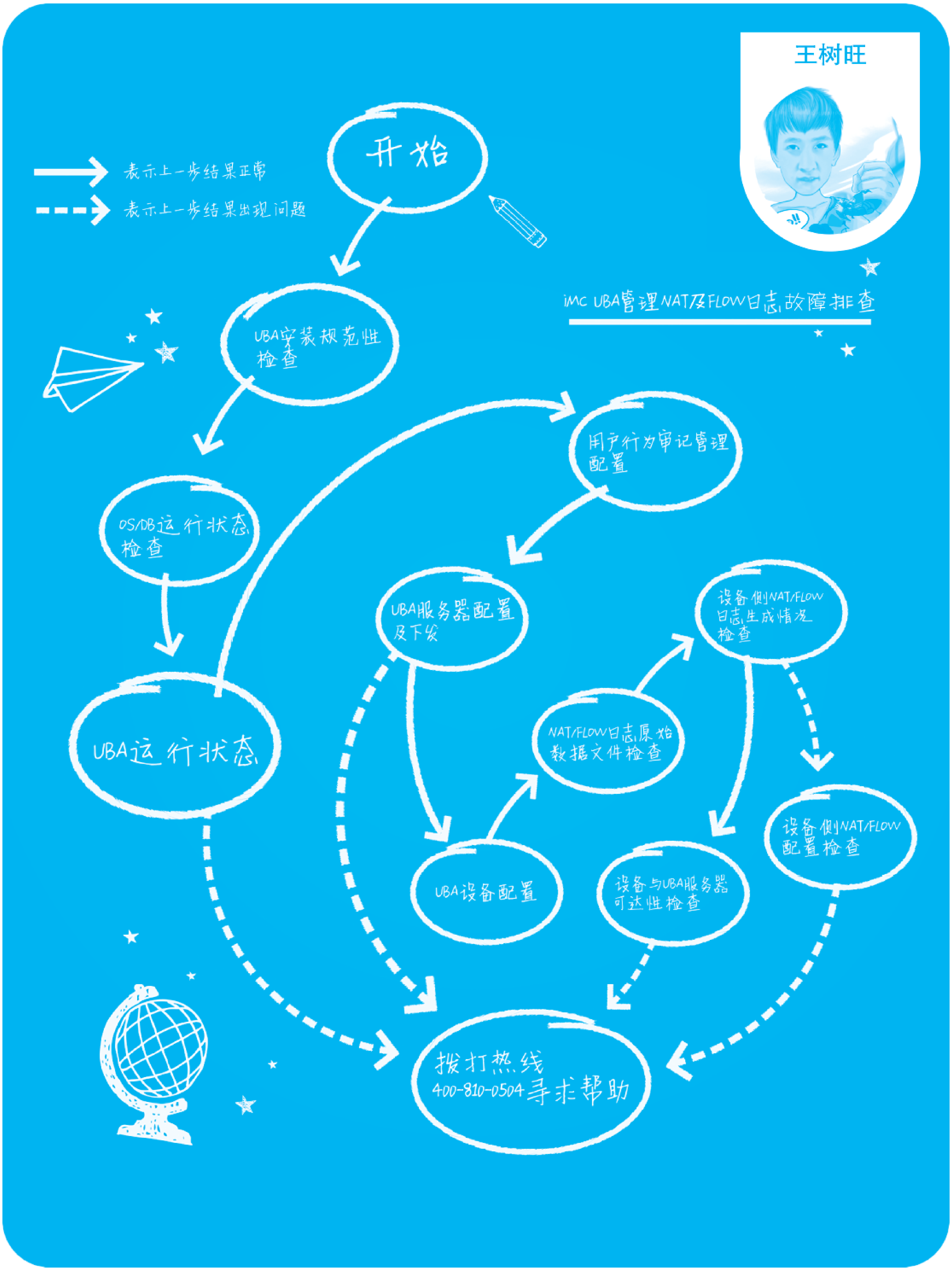
```
<Router>display ip netstream export
IP export information:
  Stream source interface                          :
  Stream destination VPN-instance                  :
  Stream destination IP (UDP)                      : 172.8.99.176 (9020)
  Version 5 exported stream number                 : 13385
  Version 5 exported UDP datagram number (failed)  : 3292 (0)
  Version 9 exported stream number                 : 0
  Version 9 exported UDP datagram number (failed)  : 0 (0)
```

（10）设备与 NTA/UBA 服务器可达性检查

检查设备与 NTA/UBA 服务器是否可达，对应的端口（如以上程序中的 9020）是否被中间的防火墙过滤等。

（11）设备侧 NetStream 配置检查

如果在前面的 display ip netstream export 环节发现没有 NetStream 日志报文发出，则需要进一步对照对应产品的配置手册排查设备版本是否正确、NetStream 相关配置是否正确。


王树旺
iMC UBA管理NAT及FLOW日志故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
UBA安装规范性检查
OS/DB运行状态检查
UBA运行状态
用户行为审记管理配置
UBA服务器配置及下发
UBA设备配置
NAT/FLOW日志原始数据文件检查
设备侧NAT/FLOW日志生成情况检查
设备与UBA服务器可达性检查
设备侧NAT/FLOW配置检查
拨打热线
400-810-0504寻求帮助

1. iMC UBA 管理 NAT/FLOW 日志问题排查

iMC UBA 用户行为审记组件可以和设备的 NAT/FLOW 日志配合进行用户行为审记。iMC UBA 管理 NAT/FLOW 日志的问题排查思路主要分为以下两大部分。

① 设备侧是否将对应终端用户的访问流量转换生成 NAT/FLOW 日志并将日志发送给 iMC UBA 服务器。

② iMC UBA 服务器收到设备侧的 NAT/FLOW 日志，缓存在本地然后写入数据库并最终展示出来。

本问题排查思路采用从结果向来源的思路编写。

2. 流程图相关操作说明

(1) UBA 安装规范性检查

对照《智能管理中心(iMC)部署和硬件配置方案》对现场 UBA 服务器的安装规范进行检查，排查现场的服务器硬件条件是否符合 UBA 服务器的安装规范要求。重点检查如下几点。

① UBA 服务器是否专机专用，即除了安装 iMC 之外不安装其他类似的网络管理类产品。

② 服务器的硬件配置符合 UBA 的安装及运行要求，此项请重点关注服务器的磁盘性能及空间的情况。

③ 在大规模场景中，UBA 服务器是否进行了合理的分布式部署。

(2) OS/DB 运行状态检查

UBA 作为一个软件产品其运行依赖于底层操作系统及数据库的正常运行，这部分重点排查的内容如下。

① 操作系统、数据库是否为正版软件。

② 操作系统、数据库是否已打上所需的补丁(对照 iMC PLAT、UBA 的版本说明书)。

③ 操作系统的系统时间配置是否正确。

(3) UBA 运行状态检查

这部分重点排查的内容如下。

① iMC 部署监控代理中各进程运行正常，无异常的进程。

② iMC UBA 服务器的 CPU、内存利用率正常。

(4) 用户行为审计管理配置

用户行为审计分为通用审计、地址转换审计、Web 访问审计、文件传输审计、邮件审计几种，请注意 NAT/FLOW 日志情况下主要用于地址转换审计。

请检查“配置管理”→“用户行为审计管理”中已经创建了对应的地址转换审计任务并检查对应的配置是否正确。

(5) UBA 服务器配置

在单击“业务”→“配置管理”→“服务器管理”→“服务器配置”命令后应有对应的服务器配置，同时查看对应的服务器配置是否正确。

在服务器管理中可以单击“配置下发”按钮测试服务器配置能否正常下发到 UBA 接收器进程上，正常情况下会显示下发成功，如图 8-268 所示。



图 8-268　UBA 服务器配置

(6) UBA 设备配置

可以在单击 iMC UBA“业务”→“配置管理”→“设备管理”→“修改设备”命令后应有对应的设备配置同时检查设备配置是否正确。请注意 SNMP 团体字指设备上配置的 SNMP 读团体字，如图 8-269 所示。



图 8-269　UBA 设备配置

(7) UBA NAT/FLOW 原始日志数据文件检查

UBA 会将收到的 NAT/FLOW 日志先缓存到本地形成文件再逐一入库，该原始日志数据文件的保存路径为 UBA 部署所在服务器安装目录的 data/processorData/data 目录，正常情况下该目录应该有待入数据库的少量原始日志文件。如果没有说明情况异常，多为配置类问题；如果有大量的日志文件也是异常的，说明原始日志文件入数据库时存在积压的情况，需要排查数据库性能、磁盘空间是否足够等方面的因素。

(8) 设备侧 NAT/FLOW 日志生成情况检查

检测设备侧是否成功地将 NAT/FLOW 日志发送给 iMC UBA 服务器，重点排查发送的目的 IP 地址、端口是否正确，是否有日志报文发送出来。

不同设备的命令行可能不太一样，但原理是相同的，下面以 SR88 设备发送 FLOW 日志为例进行举例说明。

命令：*display userlog export slot slot-number* [| { *begin* | *exclude* | *include* } *regular-expression*]

如下面程序中的 1.2.3.6 应该为 UBA 服务器的 IP 地址，对应的监听端口为 9020，同时已经成功的发送了 91 个 FLOW 日志报文。

```
<SR88> display userlog export slot 2
nat:
   No userlog export is enabled
flow:
   Export Version 3 logs to log server  : enabled
   Source address of exported logs      : 2.2.2.2
   Address of log server                : 1.2.3.6 (port: 9020)
   total Logs/UDP packets exported      : 128/91
   Logs in buffer                       : 10
```

(9) 设备与 UBA 服务器可达性检查

检查设备与 UBA 服务器是否可达,对应的 NAT/FLOW 日志发送的端口是否被中间的防火墙过滤等。

(10) 设备侧 NAT/FLOW 配置检查

如果在前面的设备侧日志生成情况环节发现没有 NAT/FLOW 日志报文发出,则需要进一步对照对应产品的配置手册排查设备版本是否正确,NAT/FLOW 相关配置是否正确。


寻尚岩
802.1x 认证故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和接入设备可达性检查
设备侧802.1x配置检查
设备侧Radius配置检查
UAM接入设备配置检查
UAM账号信息检查
检查UAM服务配置
是否证书认证
是否LDAP+PEAP+mschapv2
检查UAM/iNode客户端证书配置
iNode客户端802.1x连接检查
域控服务器侧虚拟计算机配置
UAM侧域控服务器配置检查
拨打热线400-810-0504寻求帮助

1. 开始

802.1x 协议是基于端口的网络控制协议，在认证客户端和认证设备之间采用受保护的局域网认证协议(EAPol)，现在已成为局域网接入的基本认证方式。

对于 802.1x 认证问题，定位故障的思路及顺序是：UAM 侧服务器软硬件状态及路由可达性检查、802.1x 认证基本配置检查、确认是否证书认证、证书相关配置检查。

本文举例组网如图 8-270 所示。



图 8-270　组网举例

IP 规划如下。

认证终端 PC：172.16.16.2/24，网关 172.16.16.1。

认证设备：VLAN 16：172.16.16.1/24，VLAN 100：172.16.100.1/24。

iMC 服务器：172.16.100.122/24，网关 172.16.100.1。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、同时在线人数多，则需要根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”组件是否是已部署的状态。

需要关注的组件为“用户接入管理”，其状态应为“已部署”，如图 8-271 所示。



图 8-271　“用户接入管理”状态

(2) iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程,各进程是否正常为“已经启动”。

① 在部署监控代理中,查看 uam.exe、uamjob 进程是否正常启动,如图 8-272 所示。



进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
imcwlanperfdm.exe	已经启动	本机	0	28,644	2013-07-16 09:34:35	可管理进程	自动
img.exe	已经启动	本机	0	8,232	2013-07-16 09:34:21	核心进程	自动
processor.exe	已经启动	本机	0	70,268	2013-07-16 09:34:40	可管理进程	自动
receiver.exe	已经启动	本机	0	79,744	2013-07-16 09:34:39	可管理进程	自动
tam.exe	已经启动	本机	0	14,552	2013-07-16 09:34:37	可管理进程	自动
tftpserver.exe	已经启动	本机	0	14,064	2013-07-16 09:34:11	可管理进程	自动
uam.exe	已经启动	本机	0	5,416	2013-07-16 09:34:37	可管理进程	自动
damserver	已经启动	本机	0	175,304	2013-07-16 09:33:48	可管理进程	自动
dataanalyzer	已经启动	本机	0	115,320	2013-07-16 09:33:48	可管理进程	自动
euplat	已经启动	本机	0	199,160	2013-07-16 09:33:48	可管理进程	自动
unbaserver	已经启动	本机	0	152,444	2013-07-16 09:33:48	可管理进程	自动
jserver	已经启动	本机	0.43	1,739,260	2013-07-16 11:33:27	可管理进程	手动
portalserver	已经启动	本机	0	182,100	2013-07-16 12:08:38	可管理进程	自动
webServiceNode1	已经启动	本机	0	177,944	2013-07-16 09:33:48	可管理进程	自动
webServiceNode2	已经启动	本机	0	177,064	2013-07-16 09:33:48	可管理进程	自动
cmdbserver	已经启动	本机	0	198,664	2013-07-16 09:33:48	可管理进程	自动
trmserver	已经启动	本机	0	169,272	2013-07-16 09:33:48	可管理进程	自动
uamjob	已经启动	本机	0	154,632	2013-07-16 09:33:48	可管理进程	自动
mschapv2server	已经启动	本机	0	177,304	2013-07-16 12:08:38	可管理进程	自动
dnsProxy	已经启动	本机	0	173,420	2013-07-16 09:33:48	可管理进程	自动
policyserver	已经启动	本机	0	172,552	2013-07-16 09:33:48	可管理进程	自动

图 8-272 各进程启动情况

说明:

(a) 一般情况下,这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) uamjob 功能主要是执行定时任务,uam 进程主要负责认证、计费。

② 检查服务器 1812、1813 UDP 端口是否被 uam 相关进程所监听,如图 8-273 所示。

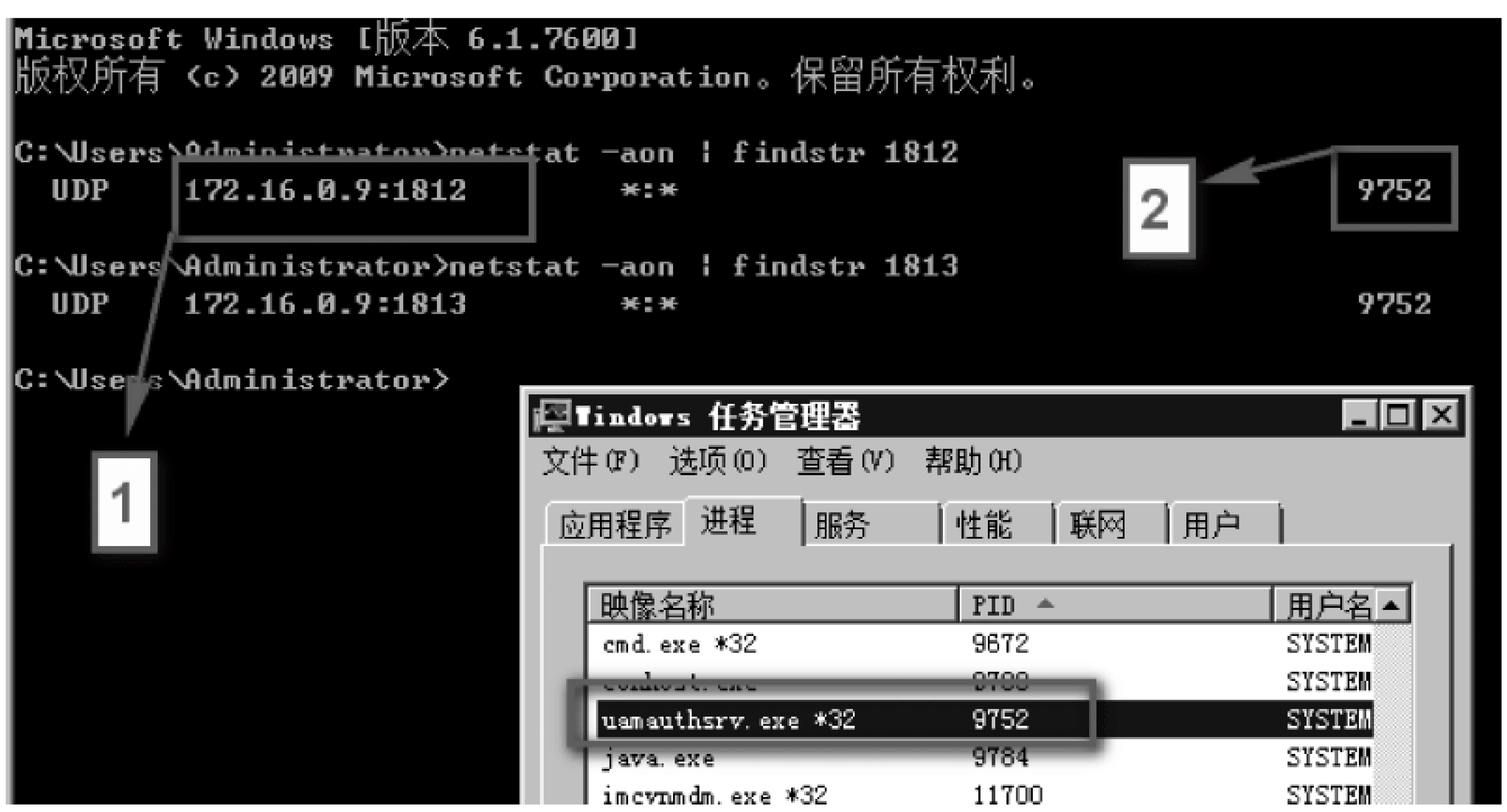


图 8-273 各端口被 uam 进程监听情况

说明:

(a) Windows 操作系统中,通过

netstat -aon | findstr :端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

(b) 1812、1813 所对应的进程 PID 应为 uam 相关的进程。

(c) 1812、1813 对应的 IP 应为 UAM 服务器实际 IP 地址。

(3) iMC 服务器和接入设备可达性检查

单击“业务”→“用户接入管理”→“接入设备管理”→“接入设备配置“命令后需添加接入设备发给 iMC 服务器 Radius 协议报文的端口 IP,iMC 默认会同该 IP 进行 Radius 协议报文交互,需保证 iMC 可以 ping 通该 IP,本例中接入设备 IP 应为 172.16.100.1,如图 8-274 所示。



图 8-274　iMC 服务器与接入设备可达性检查

说明:接入设备会有多个 IP 地址,如果要更改接入设备 IP,需在 Radius Scheme 视图下配置如下命令。

[sw-radius-h3c] nas-ip 172.16.2.1,并在 iMC 上更改为 172.16.2.1。

(4) 设备侧 802.1x 配置检查

```
[sw] dot1x
[sw] dot1x authentication-method eap/chap/pap
[sw-GigabitEthernet1/0/12] dot1x
```

说明:H3C 设备默认的认证方式为 CHAP,如果是 LDAP 账号认证,则必须将认证方式改为 PAP 或 EAP,如果是证书认证,则必须将认证方式改为 EAP。

(5) 设备侧 Radius 配置检查

```
[BAS-radius-h3c]display this
# Radius 方案配置
radius schemeh3c
server-type extended
primary authentication 172.16.100.122
primary accounting 172.16.100.122
key authenticationh3c
key accountingh3c
nas-ip 172.16.100.1
```

```
[BAS-isp-dot1x]display this
#域配置
domaindot1x
 authenticationlan-access radius-scheme h3c
 authorizationlan-access radius-scheme h3c
 accountinglan-access radius-scheme h3c
```

(6) UAM 接入设备配置检查

① 共享密钥须和接入设备配置保持一致。

② 接入设备类型：根据实际情况选择。

③ 组网方式：如果实际接入设备支持计费报文，则选择不启用混合组网，如果接入设备不支持计费报文，则选择不启用混合组网。

④ 设备 IP：默认是发给 iMC 服务器 Radius 报文的接口 IP 地址，本例中应为 172.16.100.1，如图 8-275 所示。



图 8-275　UAM 接入设备配置检查

说明：如果填写接入设备其他端口 IP 作为接入设备 IP，须在 Radius Scheme 视图下配置 nas-ip：192.168.2.1。

（7）UAM 账号信息检查

确认账号状态、绑定信息、引用的服务，并根据配置对引用的服务进行检查，如图 8-276 所示。



图 8-276　UAM 账号信息检查

说明：该步骤主要是确认账号引用的服务，对服务进行检查时即直接检查该服务。

(8) 检查 UAM 服务配置

检查 UAM 接入服务中的服务后缀是否和接入设备的 Domain、Radius Scheme 配置保持一致；检查是否引用了正确的接入规则，如图 8-277 所示。关于 iNode 客户端后缀是否添加、认证设备 Domain 配置、iMC 上的服务后缀配置对应关系可参考如表 8-2 所示。



图 8-277　检查 UAM 服务配置

表 8-2　iMC 上的服务后缀配置对应关系

iNode 认证连接用户名	设备用于认证的 Domain	设备配置相关命令	iMC 中服务后缀
X@Y	Y	With-domain	Y
		Without-domain	无后缀
X	Default Domain	With-domain	Default Domain
		Without-domain	无后缀

说明：

① 对于设备 Radius 方案中指定“user-name-format without-domain”的情况：在 iMC 接入服务中不配置服务后缀；如对应的域配置为设备的默认域，则客户端 PC 认证时可以不带后缀名，否则需要带后缀名。

② 对于 Radius 方案中指定的是“user-name-format with-domain”的情况：iMC 接入服务中必须要配置服务后缀，在使用设备默认域做认证时，客户端的用户名可以不带后缀，如不是默认域则需要用户名带后缀认证。

(9) 确认是否证书认证

直接在单击“业务”→“用户接入管理”→“接入规则管理”→“修改接入规则”命令后，可在里面查看是否启用证书认证及证书认证类型，如果不属于证书认证，则直接检查 iNode 客户端 802.1x 连接配置，如图 8-278 所示。

说明：

① 如果是证书认证，则报文加密方式必须为 EAP 形式，具体的配置方式如下。

[H3C]dot1x authentication eap

② 证书认证安全性高，配置复杂，支持冷备，不支持 Radius 逃生。

(10) 是否 AD 用户＋PEAP＋MSCHAPV2 证书认证

确认认证用户是否属于 AD 认证用户，是否采用 PEAP MSCHAPV2 证书认证，确认方式如图 8-279 所示。



图 8-278 确认证书认证情况



图 8-279 确认认证用户为 AD 认证用户情况

说明：AD 用户：仅指从微软 LDAP 服务器同步过来的用户，open LDAP 用户无须配置 PEAP 预控服务器；iMC 仅同步用户账户，并不同步用户密码。

如果不属于此种情况，则直接检查 UAM/iNode 客户端证书配置。

(11) 域控服务器侧虚拟计算机配置检查

① 虚拟计算机名称和路径检查。

虚拟计算机必须在 Computers 下新建，首先保证虚拟计算机路径正确，路径格式一般为 CN=Computername，CN=Computers，DC=XXX，DC=XXX，本例中路径的正确写法为：CN=h3c，CN=Computers，DC=CONTOSO，DC=COM；然后需保证该名称和“UAM 侧域控服务器配置检查”配置的虚拟计算机名称保持一致，如图 8-280 所示。

② 虚拟计算机密码检查。

虚拟计算机密码检查分为以下 3 个步骤。

第 1 步，从 UAM 服务器下载密码修改脚本，如图 8-281 所示。

第 2 步，确认密码修改脚本的内容，该密码需和“UAM 侧域控服务器配置”设置的虚拟计算机密码保持一致，如图 8-282 所示。

第 3 步，在域控服务器侧 CMD 下使虚拟计算机密码生效。

确认密码和名称无误后，在域控服务器 CMD 命令行下执行该脚本，执行后不能有出错提

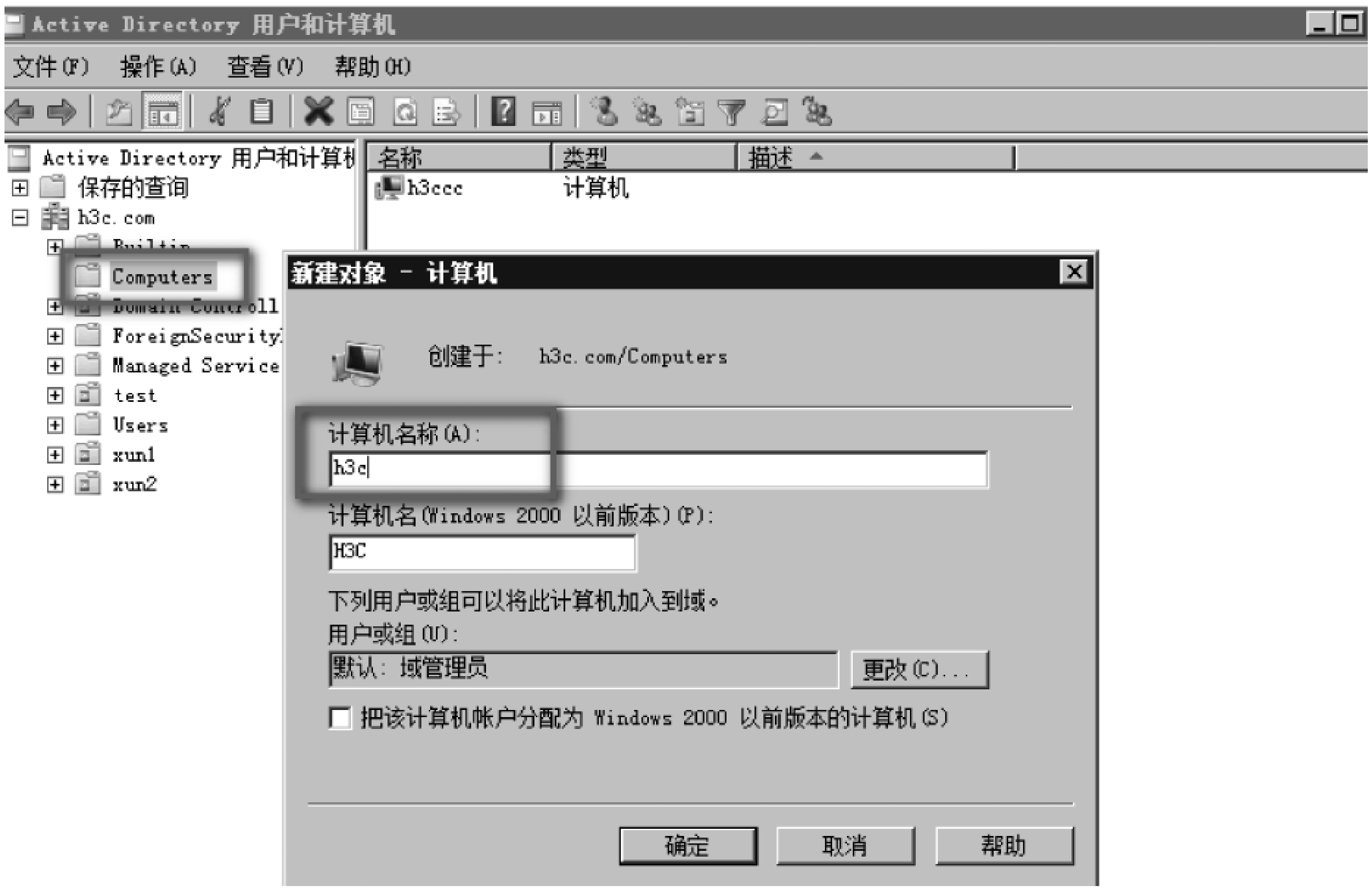


图 8-280　虚拟计算机名称和路径检查



图 8-281　修改脚本

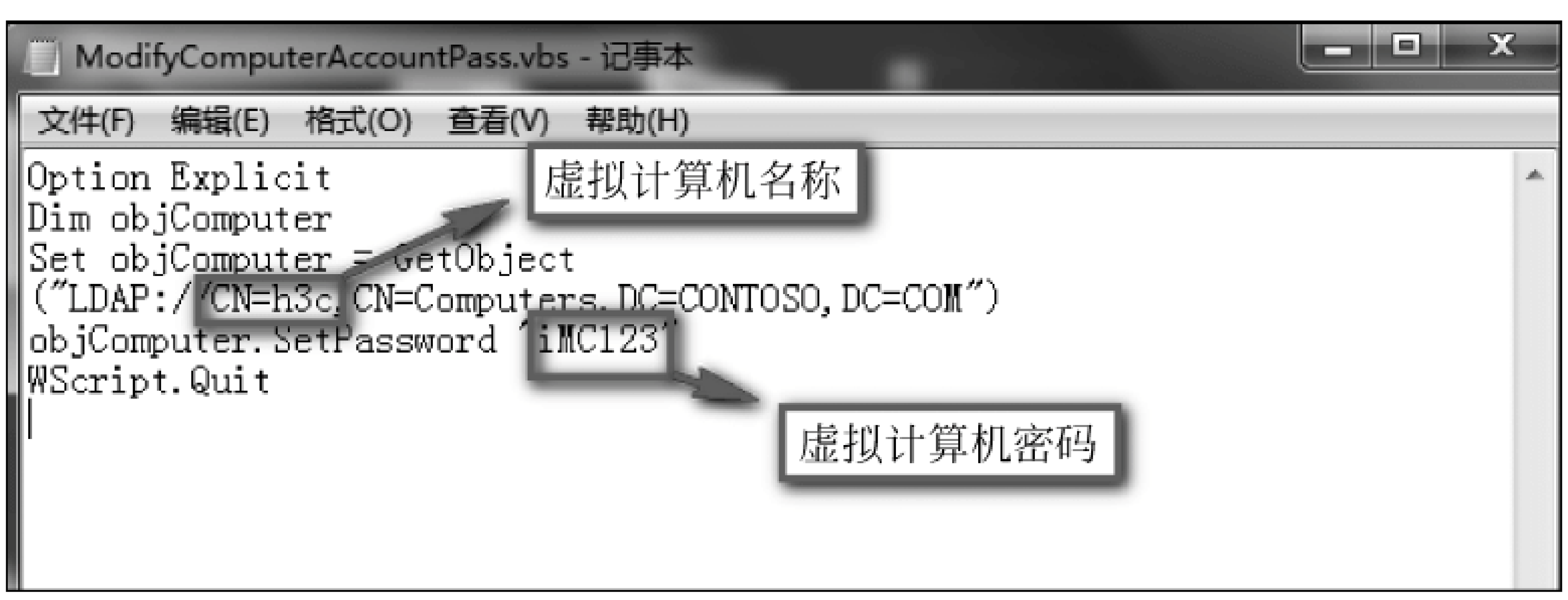


图 8-282　与虚拟计算机密码保持一致

示，如果不能保证之前是否正确执行，可再次执行该脚本，如图 8-283 所示。

(12) UAM 侧域控服务器配置检查

域控服务器全名是指 AD 服务器的计算机名称，虚拟计算机名称和密码需和“域控服务器即配置”侧的配置保持一致，如图 8-284 所示。



图 8-283 在 CMD 命令下执行脚本



图 8-284 UAM 侧域控服务器配置检查

说明：

① DNS 服务器 IP：必须填写实际 IP 地址，不能填写 127.0.0.1。

② 域控服务器 IP：必须填写实际 IP 地址，不能填写 127.0.0.1。

③ 本地服务器端口：确认不要修改此端口号。

④ 域控服务器操作系统版本：如果使用 iNode 客户端认证，则此处填写实际操作系统版本，其他情况均填写 Windows 2003 或之前版本。

虚拟计算机全名的查看方法如图 8-285 所示。

(13) 检查 UAM/iNode 客户端证书配置

① UAM 侧证书相关配置。

证书配置路径为："业务"→"用户接入管理"→"业务参数配置"→"证书配置"。

确认根证书和服务器证书是同一 CA 颁发，确认证书仍在有效期内，根证书一般为.cer 格式，服务器证书为.pfx 格式，导入证书时确认不要混淆，如图 8-286 所示。



图 8-285 虚拟计算机全名查看

② iNode 客户端证书配置，分两种情况。

(a) EAP-TLS 证书认证。

EAP-TLS 证书认证时，客户端必须安装客户端证书，默认客户端证书名称必须和接入账户名保持一致，否则会提示证书无效。

如果客户端没有根证书则不能勾选"验证服务器证书"，如图 8-287 所示。

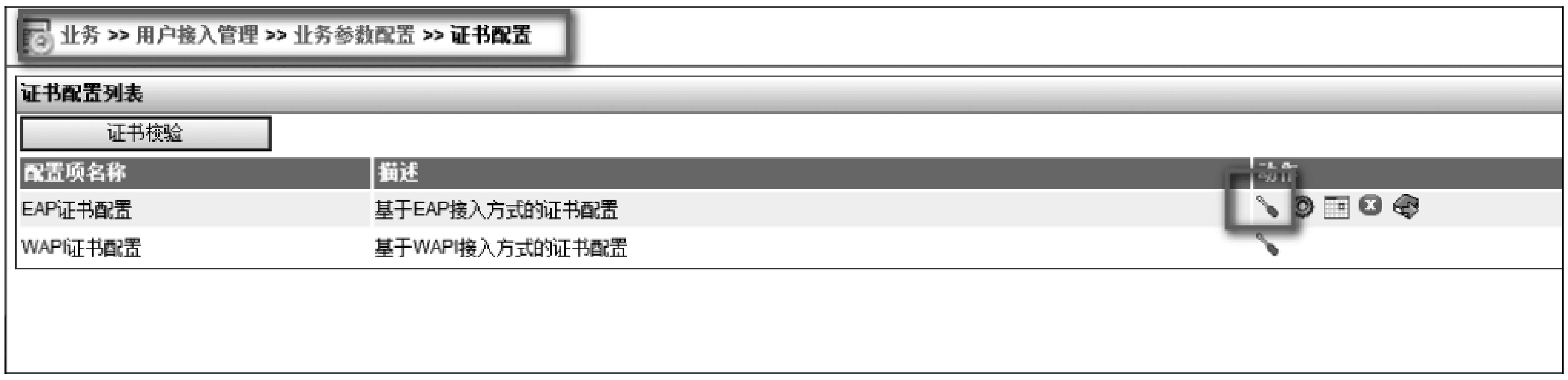


图 8-286　UAM 侧证书相关配置

（b）PEAP 证书认证。

采用 PEAP 证书认证时，客户端可以没有任何证书；客户端没有根证书时，则不能选择“验证服务器证书”单选框，如图 8-288 所示。



图 8-287　EAP-TLS 证书认证



图 8-288　PEAP 证书认证

说明：

ⓐ EAP-TLS：双向证书认证，客户端必须有客户端证书，如果不验证服务器证书，客户端可以没有根证书。

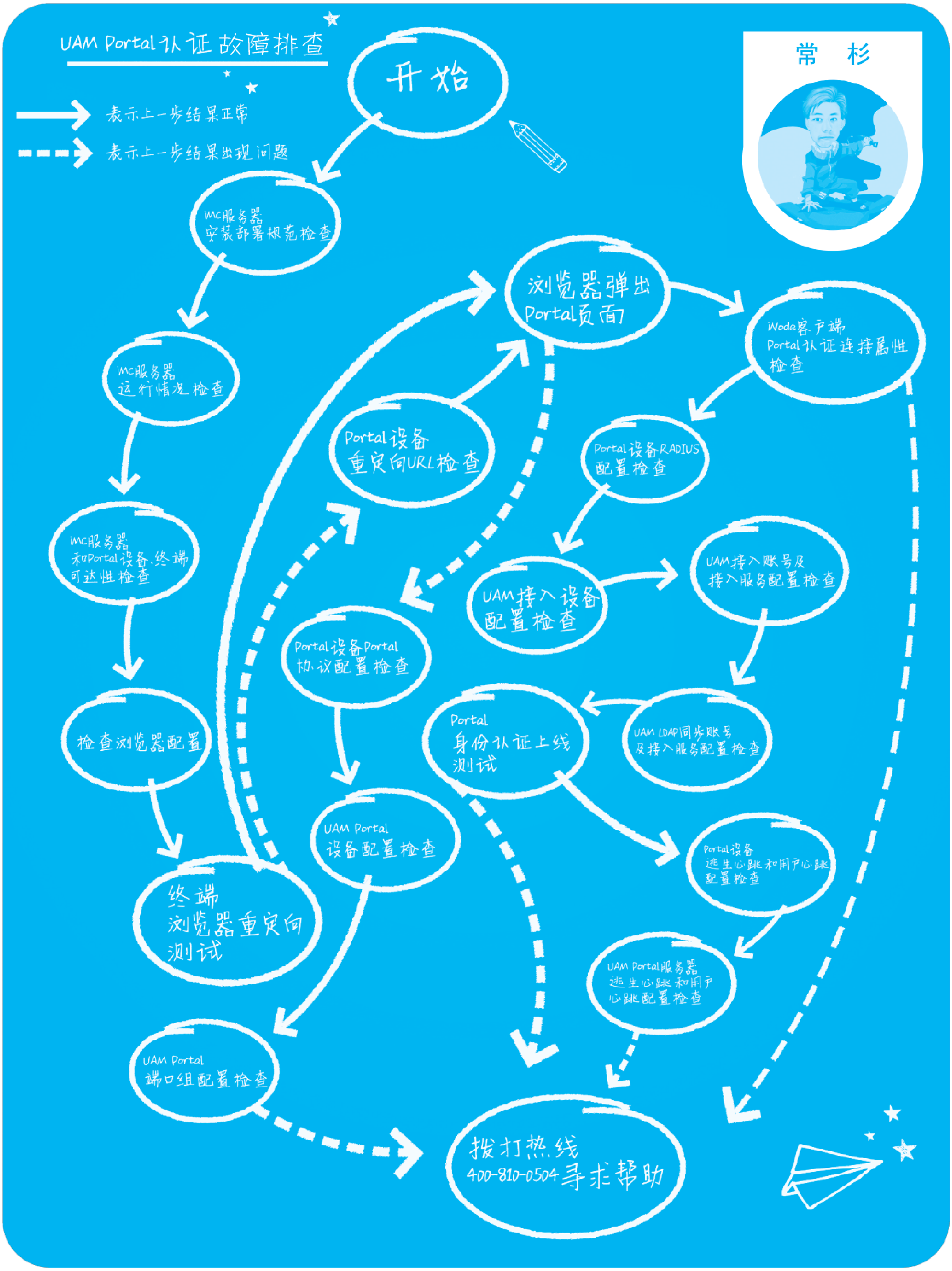
ⓑ PEAP：单向证书认证，客户端可以没有认证证书。

（14）iNode 客户端 802.1x 连接检查

iNode 客户端账号及后缀配置请参考表 8-3 的内容。

表 8-3　iNode 客户端账号及后缀配置

iNode 认证连接用户名	设备用于认证的 Domain	设备配置相关命令	iMC 中服务后缀
X@Y	Y	With-domain	Y
		Without-domain	无后缀
X	Default Domain	With-domain	Default Domain
		Without-domain	无后缀


UAM Portal认证故障排查
表示上一步结果正常
表示上一步结果出现问题
常 杉
开始
iMC服务器
安装部署规范检查
iMC服务器
运行情况检查
iMC服务器
和Portal设备、终端
可达性检查
检查浏览器配置
终端
浏览器重定向
测试
浏览器弹出
Portal页面
Portal设备
重定向URL检查
Portal设备Portal
协议配置检查
UAM Portal
设备配置检查
UAM Portal
端口组配置检查
iNode客户端
Portal认证连接属性
检查
Portal设备RADIUS
配置检查
UAM接入设备
配置检查
UAM接入账号及
接入服务配置检查
Portal
身份认证上线
测试
UAM LDAP同步账号
及接入服务配置检查
Portal设备
逃生心跳和用户心跳
配置检查
UAM Portal服务器
逃生心跳和用户
心跳配置检查
拨打热线
400-810-0504寻求帮助

1. 开始

Portal 协议简介：Portal 协议框架基于 UDP 实现，其中使用了 Radius 协议做用户身份认证，可以通过客户端或浏览器发起认证。

UAM Portal 认证排错定位思路：首先检查服务器软硬件及性能是否满足当前认证需要，然后需要从客户端或网页上线的现象来分析，相应做 iMC 服务器的检查、Portal 相关配置的检查和 Radius 相关配置的检查。

本文中举例组网如图 8-289 所示。

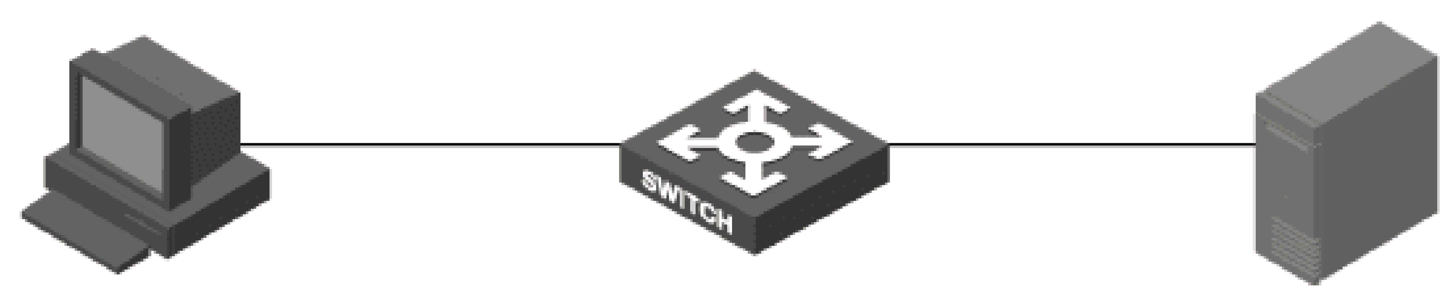


图 8-289 组网举例

IP 规划如下。

认证终端 PC：172.16.16.2/24，网关 172.16.16.1。

认证设备 H3C：VLAN 16：172.16.16.1/24，VLAN 100：172.16.100.1/24。

iMC 服务器：172.16.100.122/24，网关 172.16.100.1。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况是否符合要求。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器对应业务量的配置需求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”各组件是否是已部署的状态。

需要关注的组件有“用户接入管理”和“Portal 服务器”，其状态都应为“已部署”，如图 8-290 所示。

(2) iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程，各进程是否正常为“已经启动”。

① 打开部署监控代理，查看 uam.exe、portalserver、webServiceNode1、webServiceNode2、

uamjob 进程是否正常启动。另外，如果是网页 Portal 认证还需要确认 Portal 服务器上的 jserver/webserver 进程是否正常启动，如图 8-291 所示。



图 8-290 关注组件部署状态

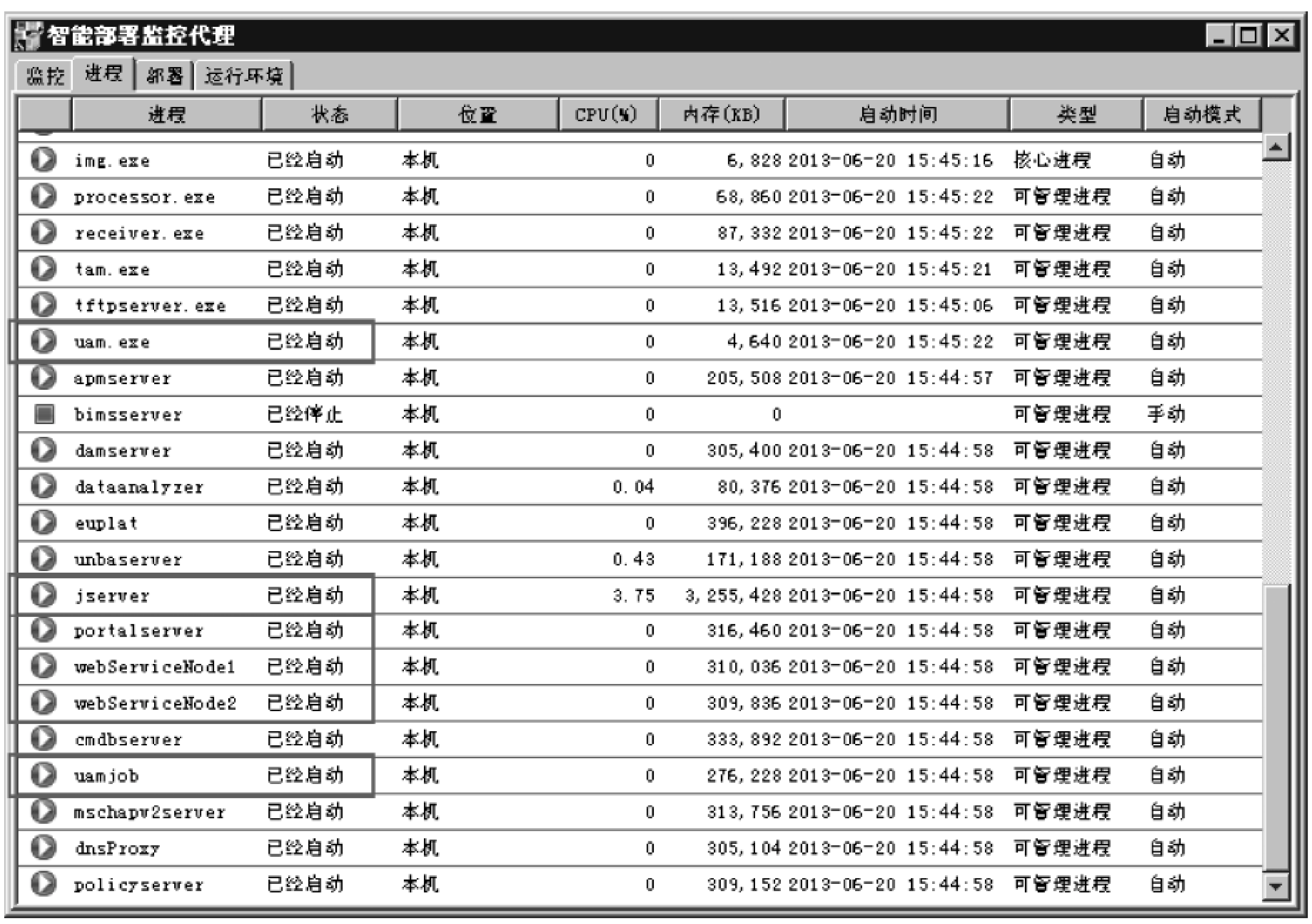


图 8-291 各进程启动情况

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) jserver 是 Portal 组件集中式部署时所需关注的进程；webserver 为 Portal 组件分布

式部署时，在从机上需要确认的进程。

② 检查服务器 1812、1813、50100、50200 UDP 端口是否被 uam 相关进程所监听，如图 8-292 所示。



图 8-292 各端口被 uam 相关进程监听情况

说明：

(a) Windows 操作系统中，通过

netstat-aon | findstr ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-293 所示。



图 8-293 命令提示符回显

其中第一列 UDP 所指监听的协议，第二列 10.153.43.100:1812 所指监听的服务器的 IP 和端口号，第三列 *：* 代表此行信息为监听状态，最右一列 8780 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，1812/1813 端口所对应的应为 uam 相关的进程，50100/50200 所对应的应为 Java 进程。

(3) iMC 服务器和 Portal 设备、终端可达性检查

Portal 认证是对上行流量的认证，并且需要和 Portal 服务器通信交互 Portal 报文。对于没有禁 ping 的环境，在认证上线之前终端 PC 是可以和 Portal 所在服务器可达的。分别从 iMC 服务器上 ping 接入设备 IP、Portal 设备 IP 和终端 IP。

对于本文的组网环境，需要分别测试 172.16.16.2 与 172.16.100.2、172.16.16.1 与 172.16.100.122、172.16.100.122 与 172.16.100.1 之间的双向可达性。

(4) 检查浏览器配置

关于认证使用的浏览器,请使用 IE 进行测试,并保证单击"Internet 选项"→"Internet 临时文件"→"检查存储的网页的较新版本"命令后选择为"自动",如图 8-294 所示。

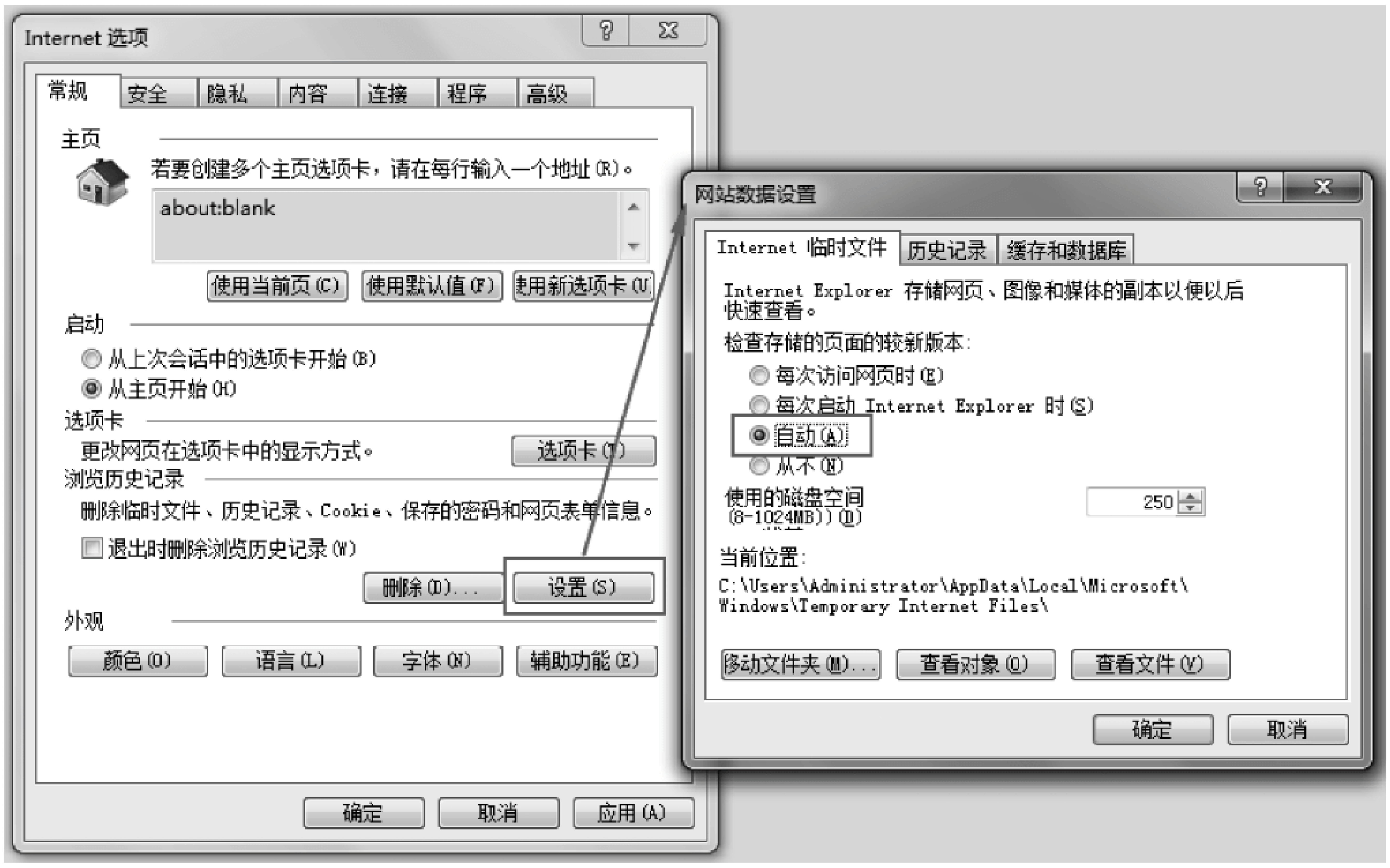


图 8-294 检查浏览器配置

说明:若此处选择"从不",浏览器会优先从本地缓存中查找网页文件的副本,终端 PC 的浏览器不向 Portal 服务器请求页面,会导致 Portal 心跳失败、认证超时掉线。

(5) 浏览器 Portal 页面跳转测试

浏览器重定向的原理:为认证上线的终端 PC 在向外发起 Http Get 请求时,网关设备会以配置好的 Portal URL 来填充地址字段,将该 Get 请求重定向到 Portal 服务器上,转而进行 Portal 认证。

打开浏览器,推荐使用 IE,在地址栏输入 IP 地址作为 URL,查看浏览器的地址栏中的 URL 是否会自动跳转成 Portal 服务器的 URL。这一步为浏览器和 Portal 设备间的配合,如果 URL 未重定向可检查设备配置。

举例:可输入 http://www.h3c.com.cn/(没有放通 DNS 地址时,请尝试 http://1.1.1.1/等地址)尝试访问,查看地址栏的地址时候会自动跳转成 Portal 的 URL。

若浏览器未发生跳转,即地址栏中的 URL 在回车访问后未发生变化,请参考对应 Portal 设备的手册,检查 Portal 设备配置中 Portal 服务器是否配置、接口中是否启用了 Portal。

```
[H3C] display current-configuration | include portal server imcportalserver
portal server imcportalserver ip 172.16.100.122 key portalkey url http://172.16.100.122:8080/portal
portal server imcportalserver method direct
```

说明:

① imcportalserver 为设备本地有效的 Portal 服务器名称,172.16.100.122 为 Portal 服务器的地址,portalkey 为 Portal 设备和 Portal 服务器交互时所用的共享密钥,http://

172.16.100.122:8080/portal 为 Portal 网页的重定向 URL。

② 对于命令 portal server imcportalserver method direct，需要详细检查其是否在认证接口上启用。

接下来查看浏览器是否正确显示了 Portal 认证页面，如有报错，需要检查 Portal 设备和 UAM 中对应的 Portal 配置。图 8-295 所示为正常显示的默认页面。

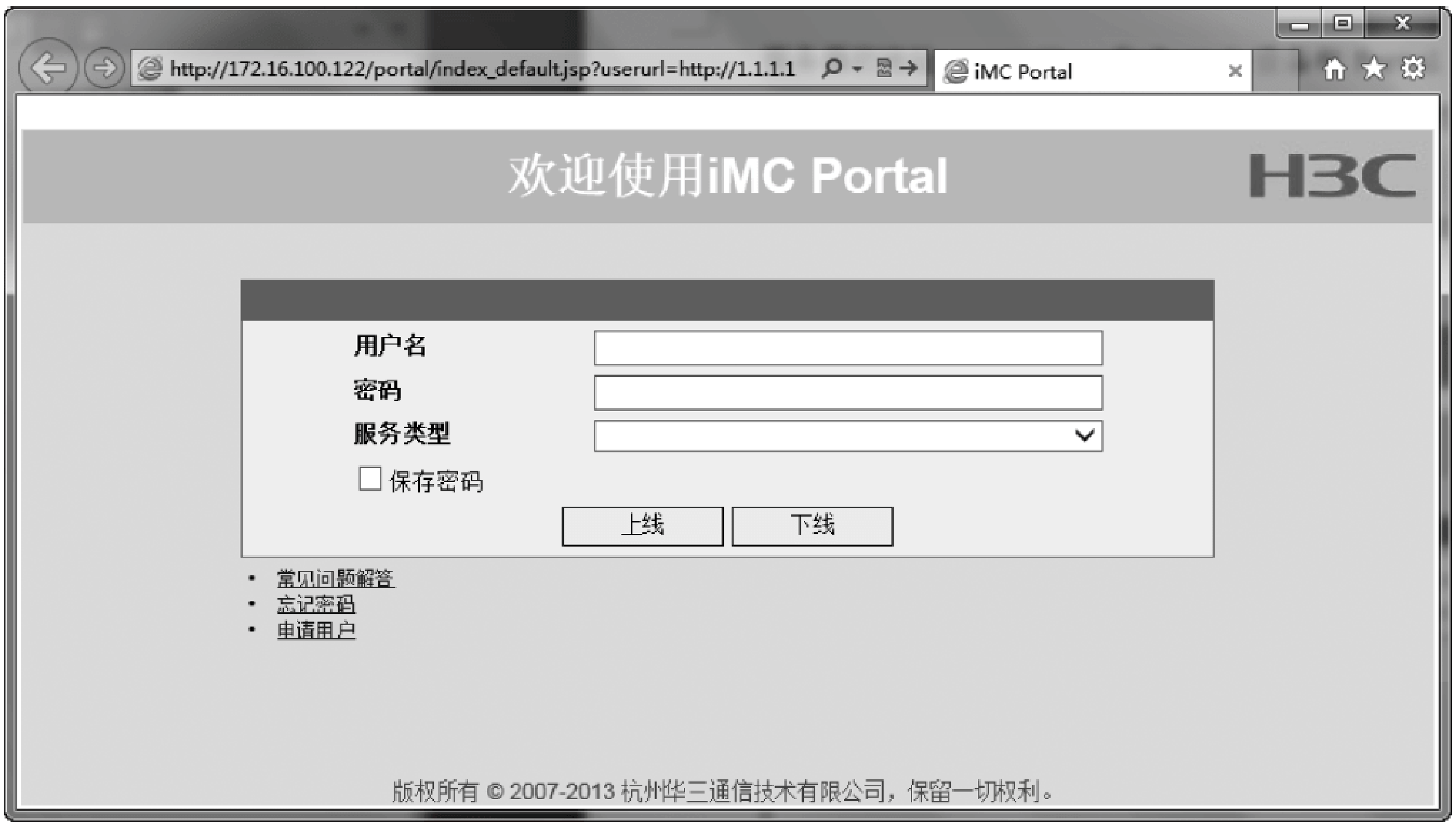


图 8-295 正常显示默认页面

（6）Portal 设备 Portal 协议配置检查

检查全局下的 Portal 配置，建议配置 portal free-rule 放通 DNS 地址的访问。

① 全局 Portal 配置举例。

```
[H3C]display current-configuration | include portal
portal serverimcportalserver ip 172.16.100.122 key portalkey url http://172.16.100.122:8080/portal
portal free-rule 0 source any destination ip 8.8.8.8 mask 255.255.255.255
portal serverimcportalserver server-detect method portal-heartbeat action permit-all interval 30 retry 2
portal serverimcportalserver user-sync interval 400 retry 3
```

说明：

（a）portal free-rule 0 命令的目的是将所有 Portal 认证区域中目的地址为 8.8.8.8（DNS 地址）的流量放通不做认证，该配置为建议配置。

（b）server-detect 的命令中配合使用 iMC 的服务器心跳，用来确保服务器出现意外宕机后，Portal 设备将 Portal 认证放开，保证用户的接入，使用参数 portal-heartbeat 来配合 iMC Portal 服务器使用，permit-all 代表 Portal 服务器失效时网关对于认证网段报文的处理方式是全部放行，检测间隔 30 秒，失败重试 2 次。

（c）user-sync 命令配合 UAM Portal 设备中用户心跳来使用，服务器定期发送所有 Portal 在线用户的列表给设备由设备将异常在线的用户踢下线。可以设置的参数有间隔时间 400 秒和重试次数 3。

② 端口中启用 portal 的配置举例。

```
[H3C-Vlan-interface16]display this
 portal server imcportalserver method direct
 portal nas-ip172.16.16.1
 portal auth-network172.16.32.0 24
```

说明：

(a) imcportalserver 为设备本地有效的全局下配置的 Portal 服务器名称，direct 参数表明这个 Portal 使用直连方式，此外还有 lay3 的三层 Portal 方式。只有配置了这条命令，Portal 才在端口上启用，为必备配置。

(b) 当启用了 Portal 网关热备，需要在启用 Portal 的三层接口上制定发送 Portal 报文的 nas-ip，对应的 iMC 中 Portal 设备添加使用此 IP 地址。

(c) 当端口上开启的端口配置为三层 Portal 的方式，需要配置好 portal auth-network 命令，以设定做 Portal 认证的网段，不配置时默认对该接口下的所有网段进行 Portal 认证，如例配置代表对源 IP 为 172.16.32.0/24 网络的终端流量做 Portal 认证。

(7) UAM Portal 设备配置检查

在单击“业务”→“用户接入管理”→“Portal 服务管理”→“设备配置”→“修改设备信息”命令后，查看是否添加 Portal 设备，该 IP 地址的配置是否与 Portal 设备上启用 Portal 的接口下的 nas-ip 所指定的地址相同。

配合本文的设备举例配置，Portal 设备的 IP 地址应为 172.16.16.1，如图 8-296 所示。



图 8-296 UAM Portal 设备配置检查

说明：监听端口默认 2000 无须更改，只是逃生心跳和用户心跳要配合 Portal 设备上的配置更改，密钥要和 Portal 设备配置一致，组网方式和 Portal 设备的配置一致。

(8) UAM Portal 端口组配置检查

需要注意的是 Portal 设备关联的地址组是否正确，在 UAM Portal 设备配置中，单击“操作”→“端口组信息管理”命令，如图 8-297 所示。

(9) iNode 客户端 Portal 认证连接属性检查

客户端会主动发出 Http 的 Get 请求来获得设备重定向的 Portal 报文，从而获取 Portal 服务器的地址。在 iNode 客户端中新建 Portal 连接时便会执行此动作。



图 8-297 UAM Portal 端口组配置检查

右击“Portal 连接”→选择“属性”命令，查看 iNode 连接属性中“网络”选项卡，确认 Portal 服务器的 IP 地址是否已自动填入，如图 8-298 所示。

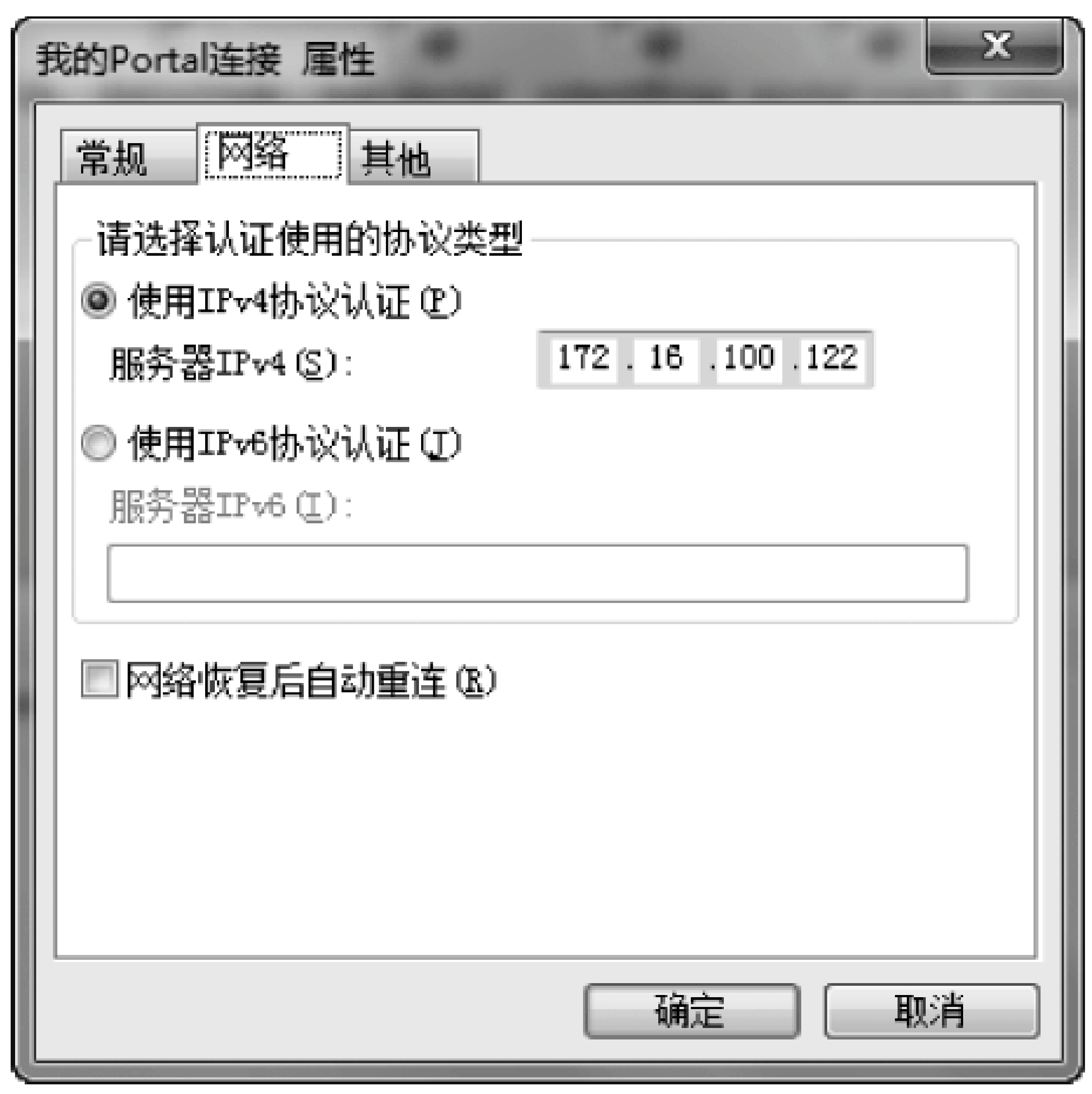


图 8-298 iNode 客户端 Portal 认证连接属性检查

说明：对于 iNode 版本低于 iNode 5.1(E0301)的 iNode PC 版本在较新版本的设备环境中使用的情况，可能会导致 iNode 客户端不能获取 Portal 服务器 IP 地址，此处不能够自动填入 Portal 服务器的 IP 地址。解决此问题需升级 iNode 客户端至 5.1(E0301)或其之后版本。

(10) Portal 设备 Radius 配置检查

Portal 协议会调用到 Radius 协议进行身份验证，相关配置举例如下。

```
[BAS-radius-radius4portal]display this
# Radius 方案配置
radius scheme radius4portal
 server-type extended
 primary authentication172.16.100.122
 primary accounting 172.16.100.122
 secondary authentication 172.16.100.123
 secondary accounting 172.16.100.123
 key authentication radiuskey
```

```
key accounting radiuskey
 nas-ip 172.16.100.1
------------------------------------------------------------
[BAS-isp-ptl]display this
# Domain 域配置
domain ptl
 authentication portal radius-scheme radius4portal
 authorization portal radius-scheme radius4portal
 accounting portal radius-scheme radius4portal
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
```

说明：

(a) 设备上的 Radius 方案配置的是主认证计费服务器为 172.16.100.122，从服务器为 172.16.100.123，认证、计费共享密钥为 RadiusKey，另外，对于设备网络复杂的情况，可使用 nas-ip 来限定 Portal 设备向 UAM 发送 Radius 报文的源 IP，user-name-format 不配置默认为 without-domain 的。

(b) Domain 配置中，认证、授权、计费类型要选择 Portal，引入了配置好的 Radius 方案。

(11) UAM 接入设备配置检查

检查设备类型和设备密钥是否配置正确，检查接入设备 IP 地址是否使用的是设备 Radius 方案中所使用的 nas-ip 值。

结合本文配置，UAM 接入设备 IP 应为 172.16.100.1。如配置错误，需要将接入设备删除再重新添加，如图 8-299 所示。



图 8-299 UAM 接入设备配置检查

(12) UAM 接入账号及接入服务配置检查

检查 UAM 接入服务中的服务后缀和 Portal 设备的 Radius 方案配置的服务后缀配置是否一致。

关于 iNode 客户端后缀是否添加、认证设备 Domain 配置、iMC 上的服务后缀配置对应关系可参考表 8-4。

表 8-4 后缀配置关系

iNode 认证连接用户名	设备用于认证的 Domain	设备配置的相关命令	iMC 中的服务后缀
X@Y	Y	With-domain	Y
		Without-domain	无后缀
X	[Default Domain] （设备上指定的默认域）	With-domain	[Default Domain]
		Without-domain	无后缀

说明：

① 对于设备 Radius 方案中指定“user-name-format without-domain”的情况：在 iMC 接入服务中不配置服务后缀；如对应的域配置为设备的默认域，则客户端 PC 认证时可以不带后缀名，否则需要带后缀名。

② 对于 Radius 方案中指定的是“user-name-format with-domain”的情况：iMC 接入服务中必须要配置服务后缀，在使用设备默认域做认证时，客户端的用户名可以不带后缀；如不是使用默认域，则需要带后缀名认证。

（13）UAM LDAP 同步账号及接入服务配置检查

对于从 LDAP 同步接入账号来做 Portal 认证的情况，需要检查 iMC 中 LDAP 相关配置和 LDAP 服务器上的相关配置，具体请参阅 UAM LDAP 排错相关篇目。

（14）Portal 身份认证测试

在浏览器或客户端输入用户名（@后缀）和密码，单击“连接”按钮。

浏览器使用地址 http://6.6.6.6/进行重定向认证，网页上线成功的页面如图 8-300 所示。

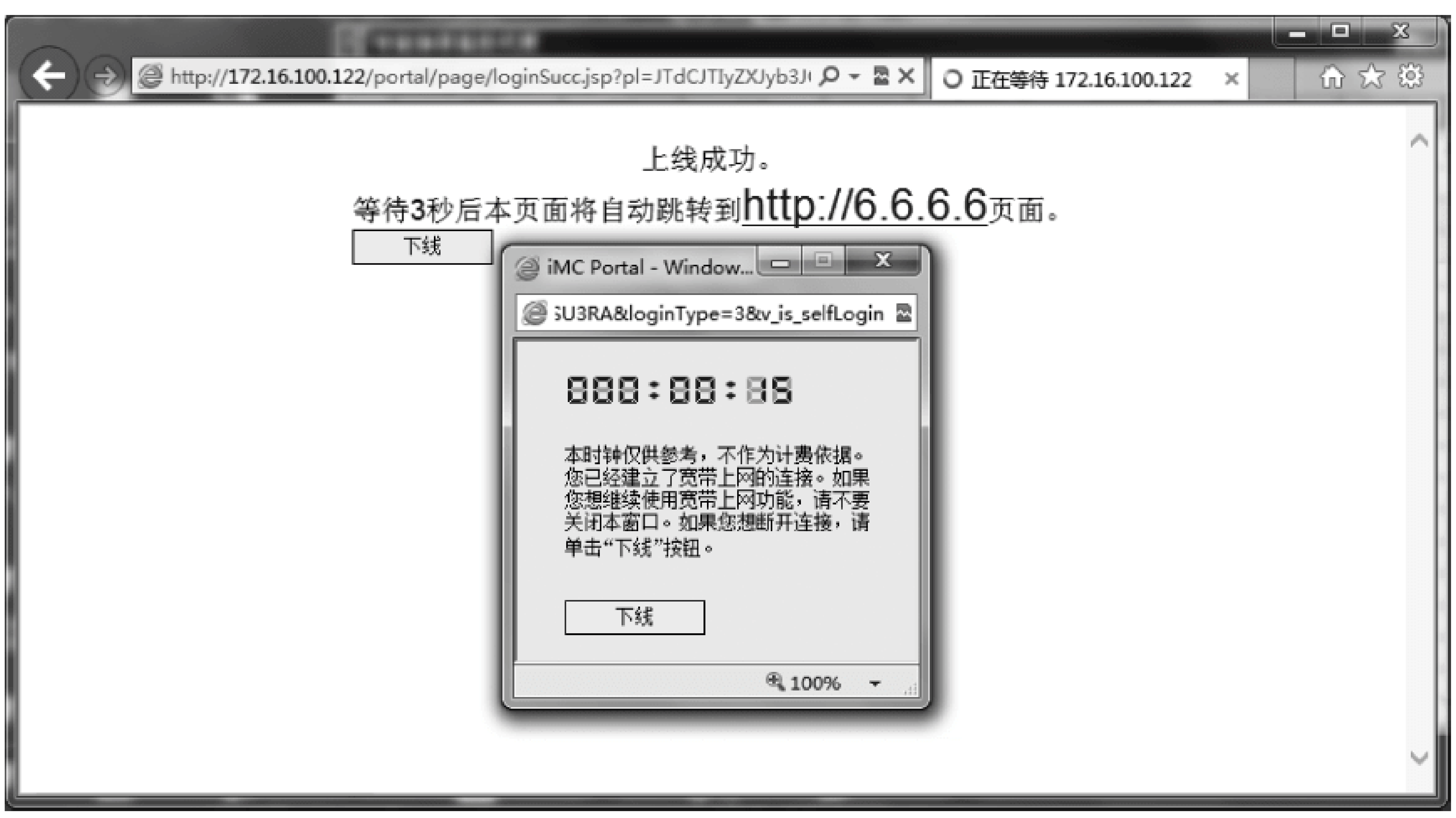


图 8-300 网页上线成功页面

客户端上线成功界面如图 8-301 所示。

（15）Portal 设备逃生心跳和用户心跳配置检查

检查设备是否支持逃生心跳和用户心跳，并且检查是否已配置逃生心跳和用户心跳的相关命令。

```
[H3C]portal server imc server-detect method portal-heartbeat action permit-all interval 30 retry 2
[H3C]portal server imc user-sync interval 400 retry 3
```

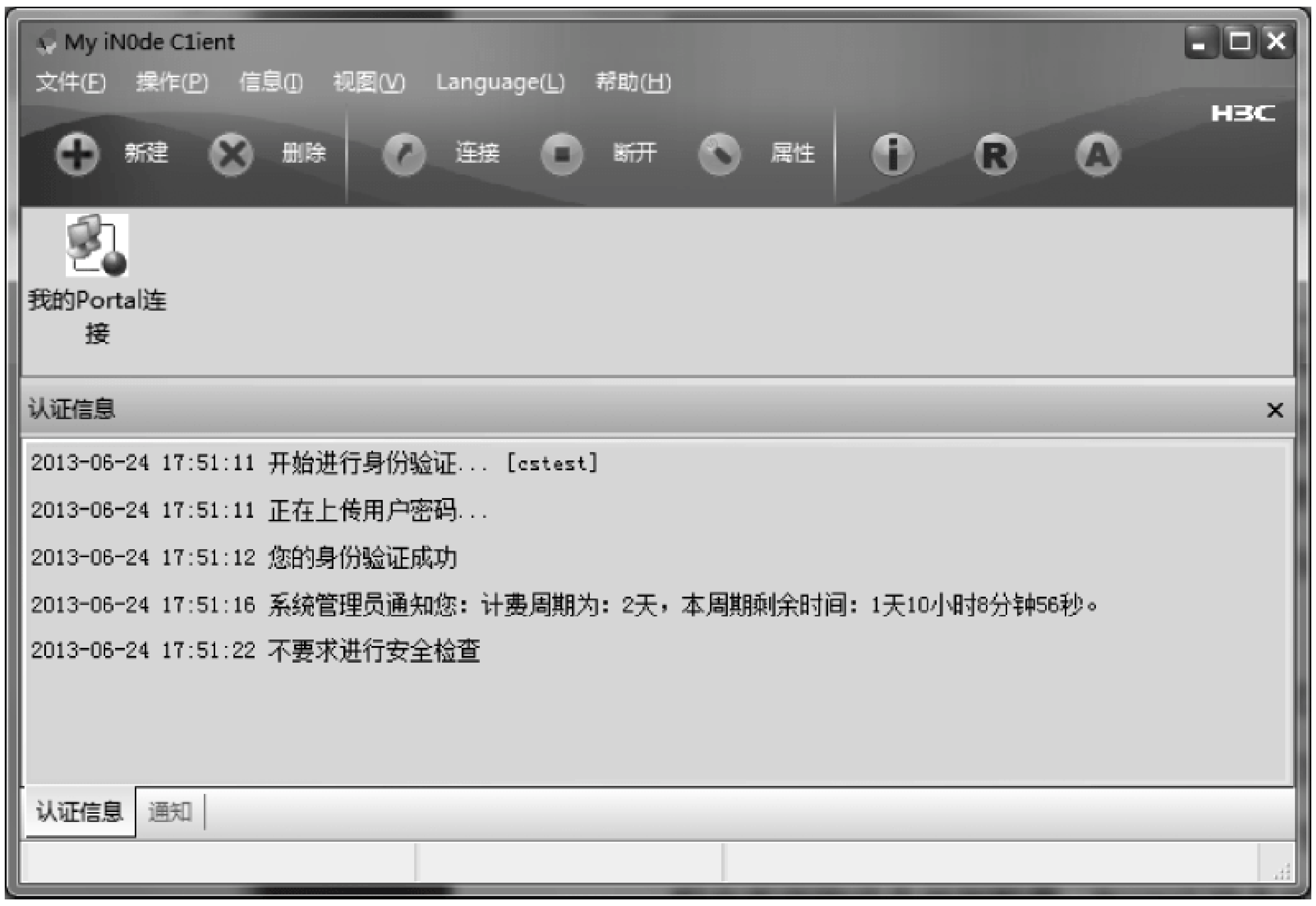


图 8-301　客户端上线成功界面

说明：如上配置已在本章 8.1.6 小节中说明，需要注意的是，设备的逃生心跳配置值应该大于服务器的发送逃生心跳的间隔时间，否则有可能出现 Portal 异常逃生的现象，同样用户心跳也需要设备配置时间超过 iMC 配置的时间。

（16）UAM Portal 服务器逃生心跳和用户心跳配置检查

该参数对应的在单击“业务”→“用户接入管理”→“Portal 服务管理”→“设备配置”→“增加设备信息”命令后有开关可以控制，需要对应 Portal 设备中命令的开启情况修改，如图 8-302、图 8-303 所示。

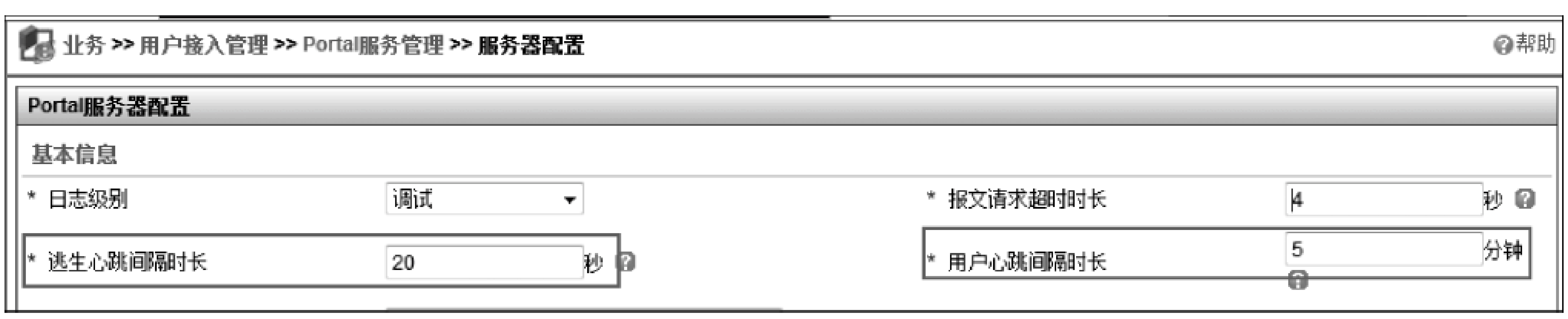


图 8-302　逃生心跳间隔时长设置

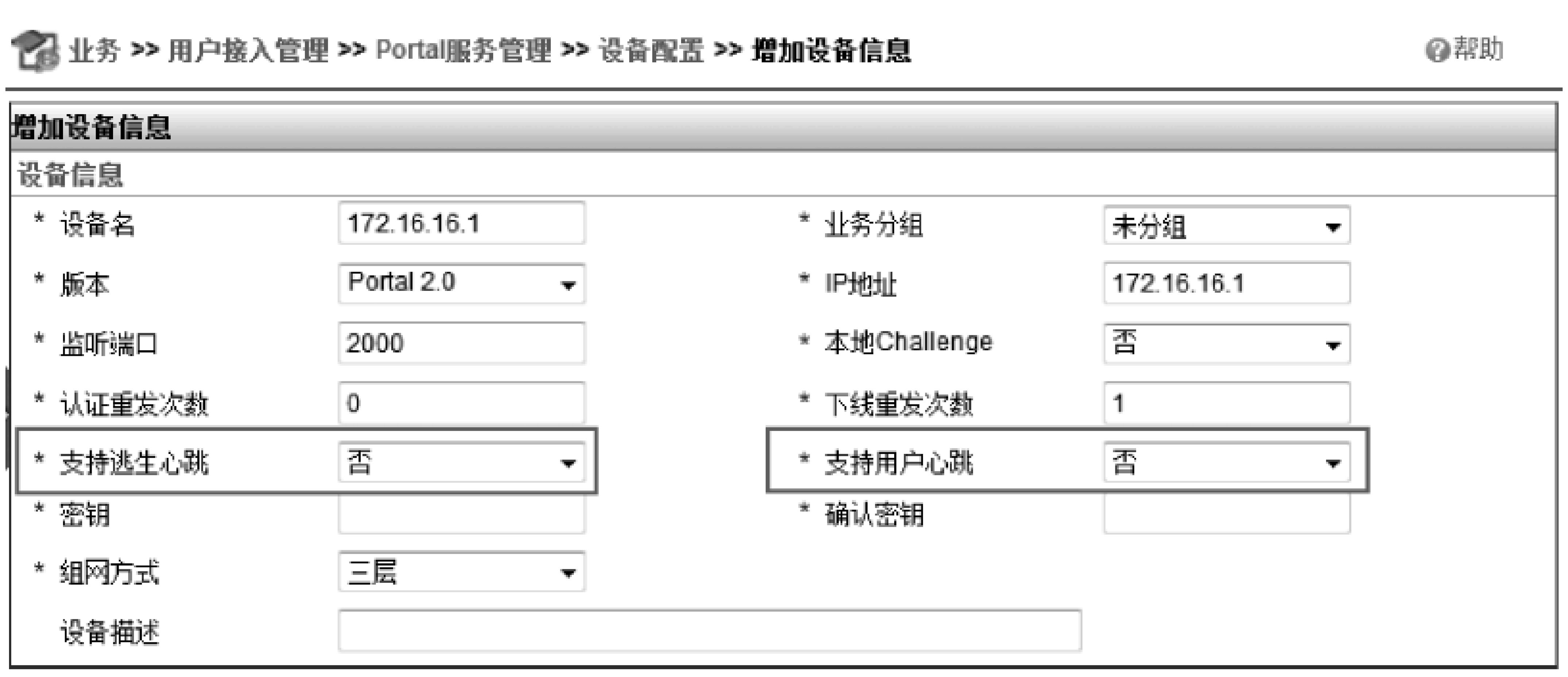


图 8-303　支持逃生心跳以及用户心跳设置

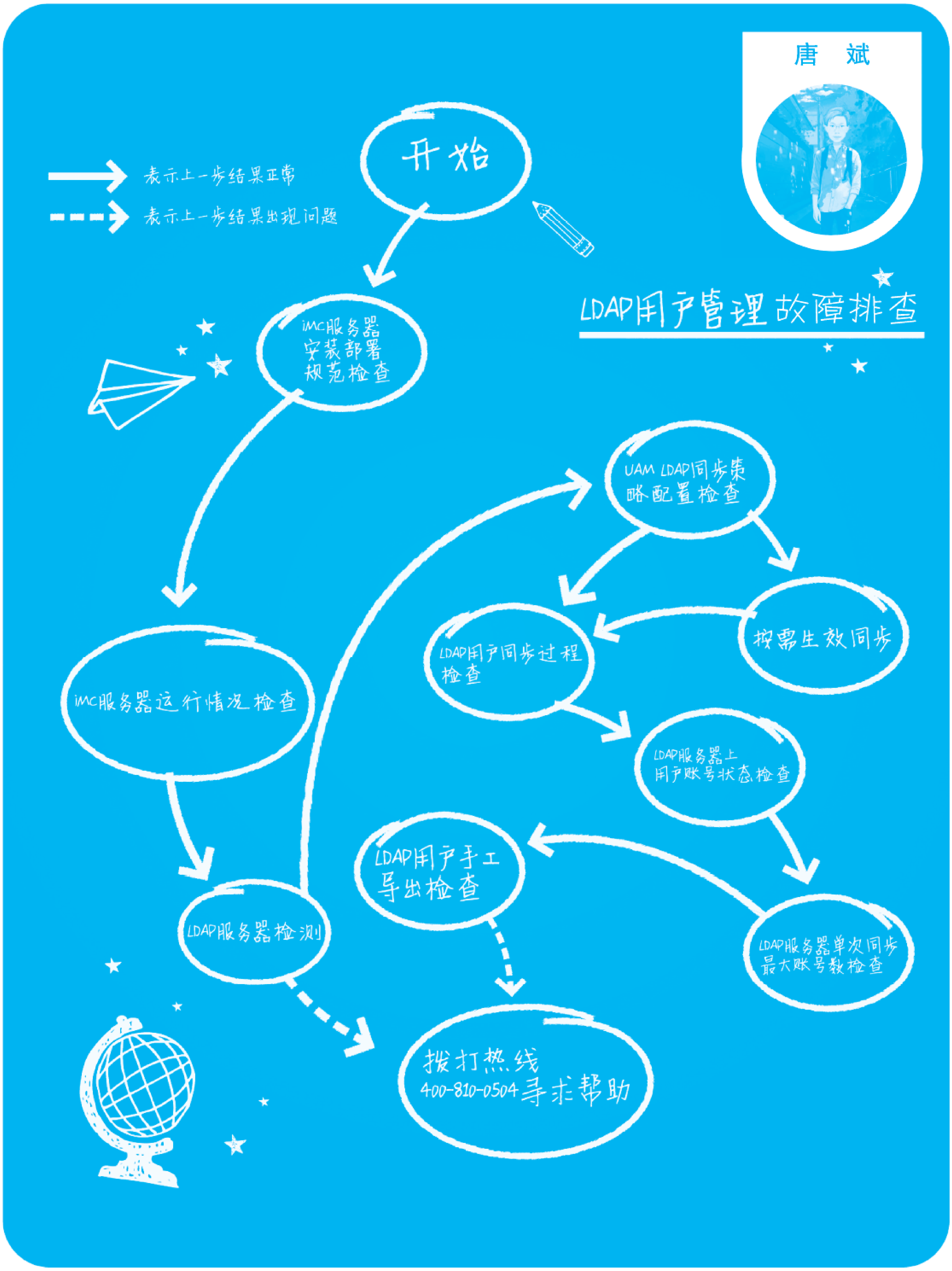
说明：

① 逃生心跳功能简介：Portal 服务器以逃生心跳间隔时长为周期，向 Portal 接入设备发送逃生心跳报文。如果设备在一定时间内没有收到逃生心跳报文（即 Portal 服务器无法正常工作）则会从认证模式切换到逃生模式。在逃生模式下，Portal 接入设备关闭认证功能，允许所有用户访问网络。如果此时设备收到逃生心跳报文（即 Portal 服务器恢复正常工作），设备会立即恢复成认证模式。

② 用户心跳功能简介：Portal 服务器以用户心跳间隔时长为周期，向 Portal 接入设备发送用户心跳报文，借此通知设备 Portal 服务器中用户的状态，并同步 Portal 服务器和设备中的用户（两边同时存在的用户将继续在线，其他用户将被下线）。

③ 逃生心跳和用户心跳的开关在 Portal 服务管理下的设备配置中，两个心跳的间隔时长在 Portal 服务管理下的服务器配置中可配置。

④ 注意这两个心跳需要配合设备使用。


唐　斌
LDAP用户管理故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
LDAP服务器检测
UAM LDAP同步策略配置检查
按需生效同步
LDAP用户同步过程检查
LDAP服务器上用户账号状态检查
LDAP服务器单次同步最大账号数检查
LDAP用户手工导出检查
拨打热线 400-810-0504寻求帮助

1. 开始

故障定位思路：检查 iMC 部署以及 iMC 运行状况，然后保证 iMC 服务器与 LDAP 服务器的网络可通。检查 UAM LDAP 服务器的配置，查看 LDAP 服务器配置的正确性。根据同步策略是否按需同步，进行进一步的排查。若非按需同步，可通过查看 iMC 上 LDAP 用户的同步状况，LDAP 服务器上账号状态进行故障排查。若为按需同步，确认策略生效后，可通过在 iMC 上导出 LDAP 服务器上的账号的方式排查 LDAP 服务器侧的问题。

2. 流程图相关操作说明

（1）iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”各组件是否是已部署的状态。

需要关注的组件有用户管理相关组件，其状态都应为“已部署”，如图 8-304 所示。



图 8-304　相关组件部署状态

（2）iMC 服务器运行情况检查

查看部署监控代理进程状态，必须都为已启动状态，如图 8-305 所示。

（3）LDAP 服务器连通性检测

① 可单击“检测”按钮以检查与 LDAP 的可达性。正常状态如图 8-306 所示，若不正常则检查下一块配置。

② 检查底层链路和路由网络，保证 iMC 服务器可与 LDAP 服务器通信。LDAP 用户需要从 LDAP 服务器同步数据，可通过 iMC 服务器与 LDAP 服务器互 ping 测试两者的网络连

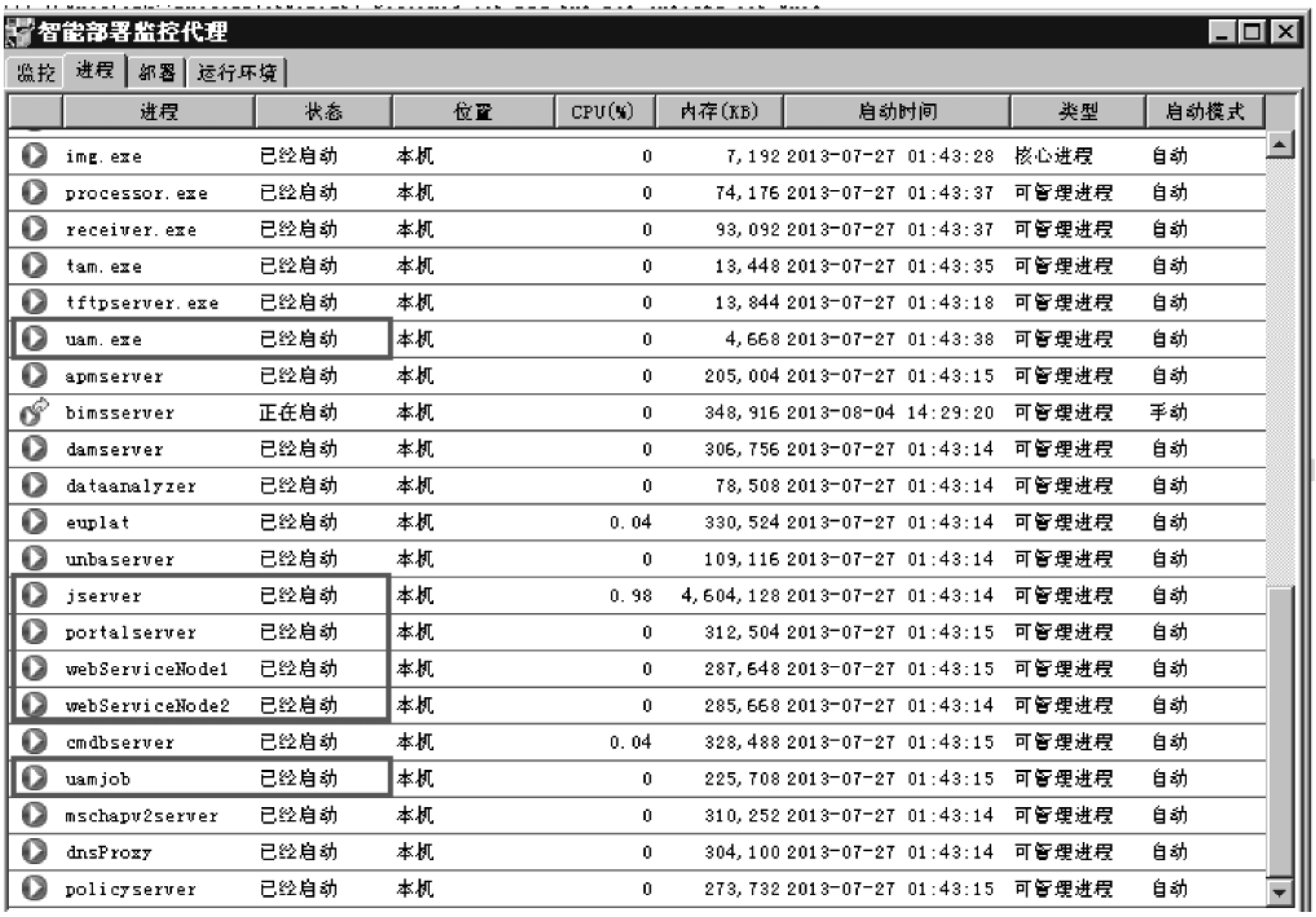


图 8-305　进程启动状态



图 8-306　正常状态

通性。由于 LDAP 普通连接方式使用端口为 TCP 389，SSL 连接方式使用端口 TCP 636。可通过“telnet 目标 ip 对端 port”，测试对端的 TCP 上的该 port 是不是处于监听状态。

说明：Windows 操作系统中，通过

telnet 目标ip 端口号

命令来显示对端某一端口的状态是否处于监听状态。

端口可用的情况如图 8-307 所示。输入 telnet 命令后回车建立 TCP 连接。



图 8-307　端口可用情况

从网卡抓包中可以看到 TCP 连接的建立。其中 ldap 为 LDAP 服务器端口 389，如图 8-308 所示。

Protocol	Info
TCP	54144 > ldap [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	ldap > 54144 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	54144 > ldap [ACK] Seq=1 Ack=1 Win=64240 Len=0

图 8-308 TCP 连接建立

③ UAM LDAP 服务器配置检查。主要检查服务器 IP 地址、端口，以及 Base DN、管理员 DN 格式是否正确。实际使用的是主服务器还是备服务器。服务器 IP 地址填入为 LDAP 的地址、端口为 LDAP 服务器监听端口，如图 8-309 所示。



图 8-309 UAM LDAP 服务器配置检查

说明：

(a) DN(Distinguished Name)为区别名称，Base DN、管理员 DN 中填写内容含义如下。CN(Common Name)为普通账号、OU(Organizational Uint)为组织单元、DC(Domain Component)域名。

(b) 对于 AD 域，若管理员账号存在于 Users 中，则管理员 DN 格式多为：CN＝XX，CN＝Users，DC＝XX，DC＝Com。

(4) UAM LDAP 同步策略配置检查

对同步策略配置进行检查，主要注意子 Base DN 的正确性和过滤条件填写的规范性。另外，请注意该条策略的同步方式是否为自动同步，是否为按需同步。自动同步的策略，会周期进行账号信息的同步。按需同步的策略，账号同步时只是预同步，并不在配置台中注册账号信息。当有账号进行认证时，方才在配置台上注册账号信息，如图 8-310 所示。

说明：

① 参数含义可在右上角“帮助”中查看。其中子 Base DN、过滤条件是限定同步策略范围的参数。多个过滤条件可以组合查询，每个过滤条件使用“()”括起来，同时在所有过滤条件前加上“&”“|”“!”来分别表示各个过滤条件之间的与、或、非关系，最后整个过滤条件使用“()”括起来。



图 8-310　UAM LDAP 同步策略配置检查

② 自动同步：每天凌晨(iMC 服务器时间)自动同步。

③ 按需同步：iMC UAM 系统中不存在、而 LDAP 服务器中存在的用户进行接入认证时，UAM 自动将认证请求转给 LDAP 服务器进行校验。如果用户通过认证，系统将自动将此用户从 LDAP 服务器同步到 iMC 中。需要注意的是，如果 iMC 中用户相关的 License 已达授权数量的上限，则无法进行同步，同时强制用户下线。

(5) 按需同步生效

若为按需同步策略，需单击“按需同步生效”按钮。该功能可以使所有状态为“有效”的按需同步策略生效，如图 8-311 所示。



图 8-311　按需同步生效

(6) LDAP 用户同步过程检查

对于同步策略，若现场条件允许，可手工单击“同步”按钮。

正常情况下，单击“同步”按钮后，显示同步策略同步已经完成，同步用户共 X 个，共成功同步 X 个用户，0 个用户同步失败，如图 8-312 所示。



图 8-312　LDAP 用户同步过程检查

查看同步结果，如图 8-313 所示，若有报错，根据错误日志进行排查。

例如：图 8-314 所示报错信息就是为与 LDAP 服务器连接问题。



图 8-313　同步结果

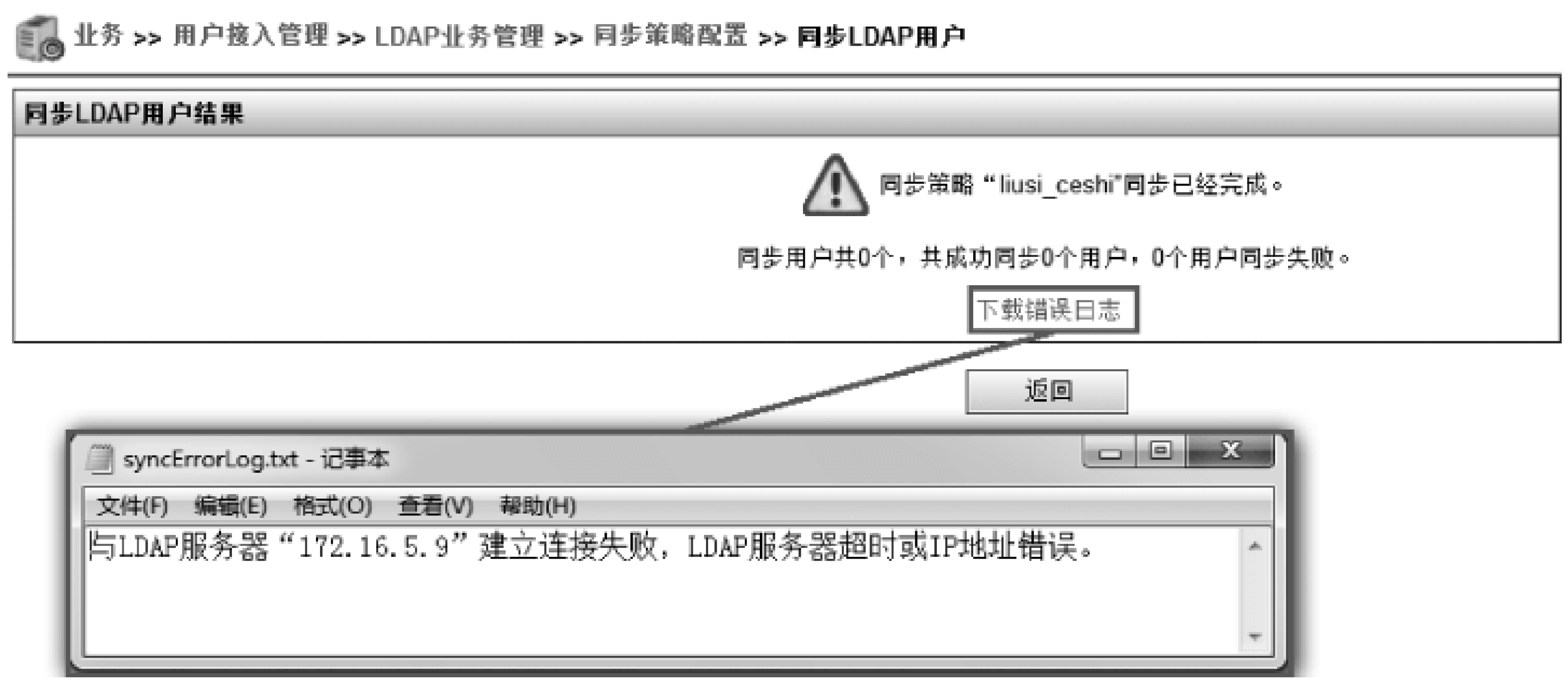


图 8-314　报错

说明：

① 若同步策略中的账号过多，则同步需要的时间较长。

② 对于按需同步的策略，同步成功后不会在 iMC 上生成 LDAP 账户，只有当该账号认证接入时才会在 iMC 上生成账户。

(7) LDAP 服务器上用户信息账号状态检查

若账户未同步成功，多数有两种情况。

则查看 iMC 上普通账户中是否已存在该账户(错误日志中会有提示，如图 8-315 所示)，同名账号无法被同步。若 iMC 已有该账号，可将已有的删除后再同步。

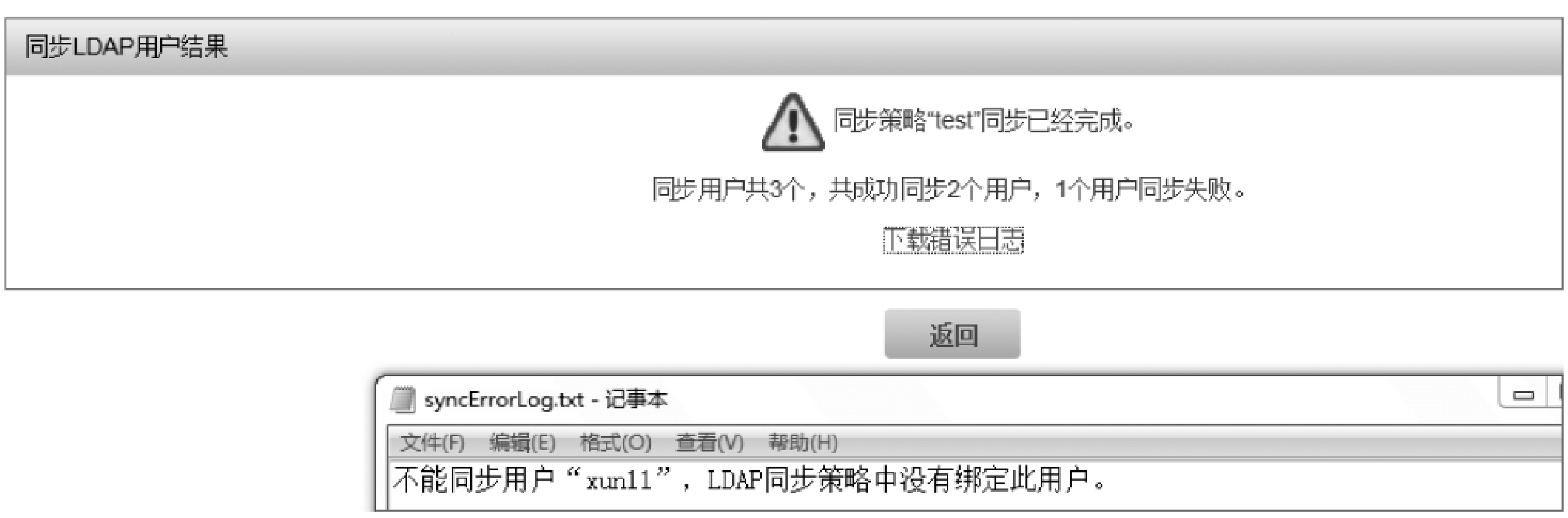


图 8-315　账户未同步成功

LDAP 服务器上是否该账号不在同步范围内(无错误提示，只能查看 LDAP 服务器该账号信息)。若不在同步范围内则调整同步策略管理范围的配置。

(8) LDAP 服务器单次同步最大账号数检查

当同步账户时，所有账户都不能同步成功，则可查看同步策略包含的账号数量是否已经超过了 LDAP 服务器一次同步账户的数量限制。若超过限制，可通过对 LDAP 同步数量限制进行修改。

说明：

① 查看及修改LDAP服务器单次同步数量的方法

可参看kms：18474。

② 检查方法

(a) 在“开始”→“运行”→“输入”下输入：ntdsutil，回车。

(b) 输入：ldap policies，回车。

(c) 输入：connections，回车。

(d) 输入：connect to domain 当前域名。

(e) 连接提示出现后，输入：quit，回车。

(f) 输入：show values，确认当前的最大返回数(默认是1000)。

③ 修改方法

(a) 输入：set maxpagesize to 10000，将最大返回数改为10000(最大返回数可以根据实际情况自行定义)。

(b) 再度输入：show values，确认当前的最大返回数(显示为：1000(10000))。

(c) 输入commit changes以确认修改。

(d) 再次输入：show values，确认当前的最大返回数为10000。

(e) 输入：quit，退出设置状态。

(f) 输入：quit，退出当前命令。

(g) LDAP用户手工导出检查。

若以上步骤中检查都无异常，可将LDAP账号导出为文本，查看其中账号信息是否正确。若导出的数据异常则可能是LDAP服务器问题，如图8-316所示。



图8-316　将LDAP账号导出为文件

导出文件设置界面如图8-317所示。

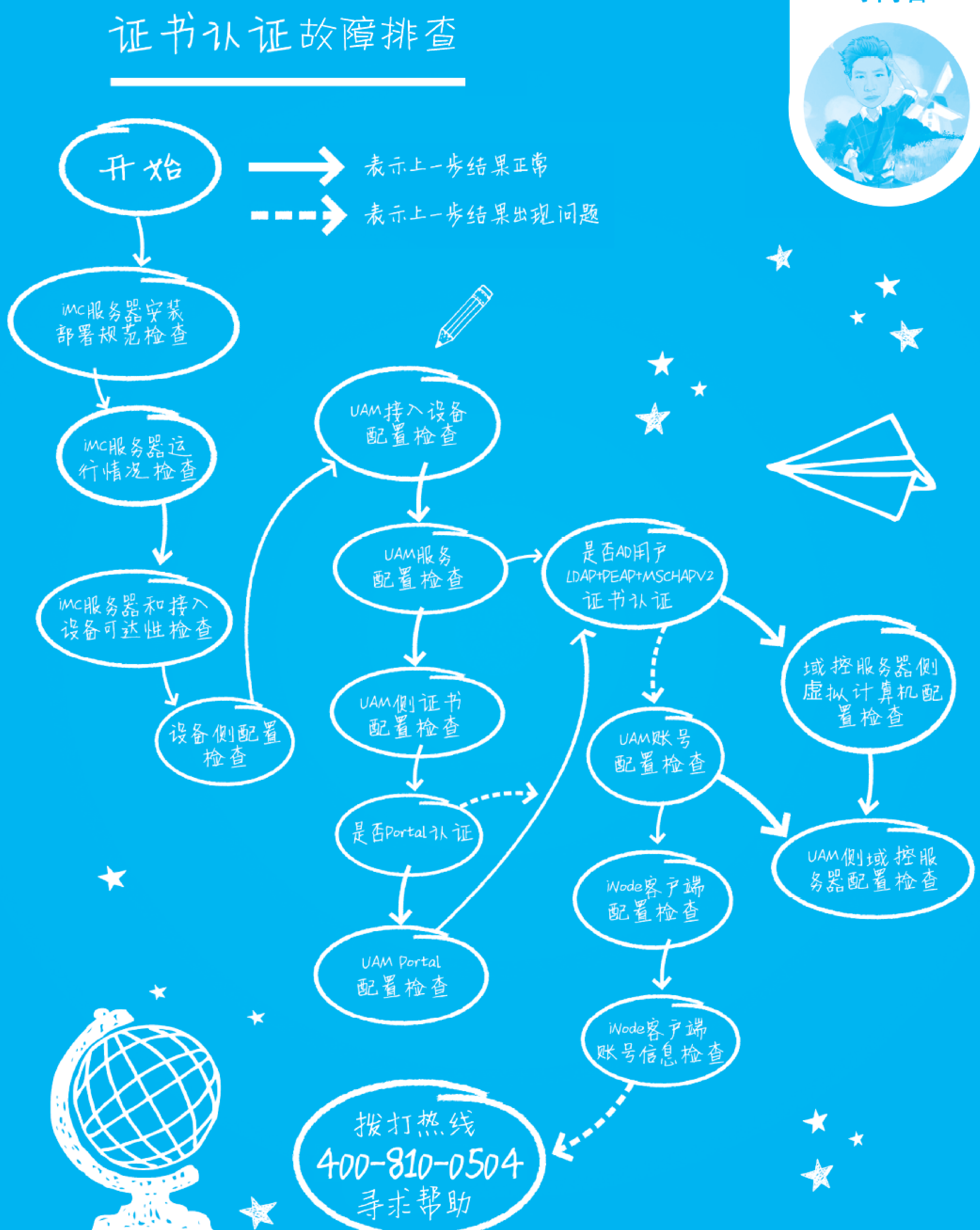


图8-317　导出文件设置界面

导出信息应注意的关键信息点如下。

displayName(对应iMC中的用户名)、sAMAccountName(对应iMC中的账号名)、distinguishedName(账号在LDAP中路径)。

寻尚岩


证书认证故障排查
开始
表示上一步结果正常
表示上一步结果出现问题
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器和接入设备可达性检查
设备侧配置检查
UAM接入设备配置检查
UAM服务配置检查
UAM侧证书配置检查
是否Portal认证
UAM Portal配置检查
是否AD用户LDAP+PEAP+MSCHAPV2证书认证
域控服务器侧虚拟计算机配置检查
UAM账号配置检查
UAM侧域控服务器配置检查
iNode客户端配置检查
iNode客户端账号信息检查
拨打热线
400-810-0504
寻求帮助

1. 开始

证书认证(支持 802.1x 和 Portal)是通过在 Radius 服务器和认证终端之间传递一系列安全参数并建立一个 VPN 隧道,然后在这个隧道内安全传递认证信息的过程。对于证书认证问题,定位故障的思路及顺序是:UAM 侧服务器软硬件状态及路由可达性检查、设备侧认证配置检查、UAM 侧认证配置检查、iNode 客户端配置检查。

本文举例组网如图 8-318 所示。



图 8-318 组网举例

IP 规划如下。

认证终端 PC:172.16.16.2/24,网关 172.16.16.1。

认证设备:VLAN 16:172.16.16.1/24,VLAN 100:172.16.100.1/24。

iMC 服务器:172.16.100.122/24,网关 172.16.100.1。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素,所以排查问题是首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格,如果认证数量大、同时在线人数多,则需要根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高,内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求,操作系统是否是高性能的 x64 版本。

② 打开部署监控代理,在部署监控代理中查看部署页面,"用户接入管理"组件是否是已部署的状态。

需要关注的组件为"用户接入管理"及"Portal 接入管理",其状态应为"已部署",如图 8-319 所示。

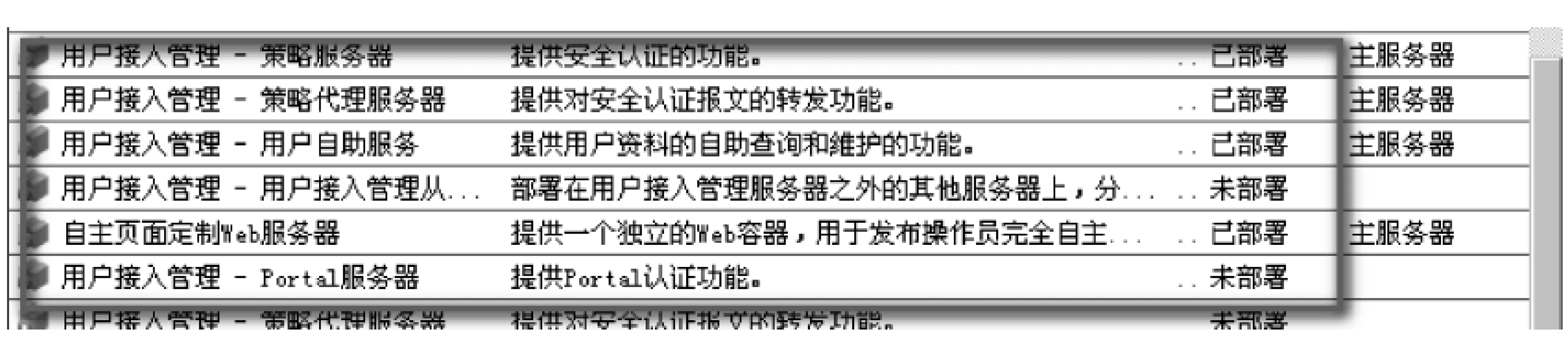


图 8-319 各组件部署状态

（2）iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程，各进程是否正常为“已经启动”。

① 在部署监控代理中，查看 uam. exe、uamjob、mschapv2server、portalserver 和 policyserver 进程是否正常启动，如图 8-320 所示。

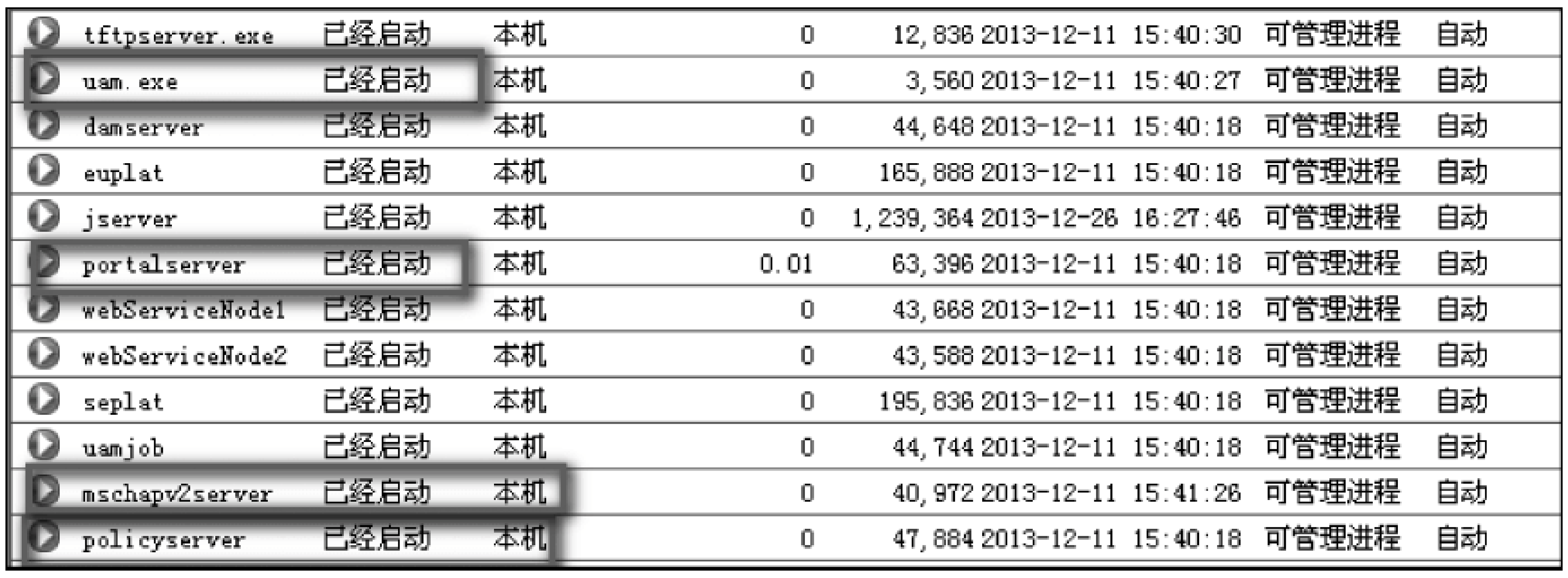


图 8-320　各进程启动情况

说明：

（a）一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

（b）uamjob 功能主要是执行定时任务，uam 进程主要负责认证、计费。

（c）potalserver 进程负责 Portal 认证，mschapv2server 进程负责 PEAP-MSchapv2 认证，policyserver 为策略服务器进程。

② 检查服务器 1812、1813、50200、9019 UDP 端口是否被 iMC 相关进程所监听，如图 8-321 所示。



图 8-321　各端口被 iMC 进程监听情况

说明：

（a）Windows 操作系统中，通过

netstat -aon | findstr ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

（b）1812、1813、50200、9019 所对应的进程 PID 应分别为 uamauthsrv.exe、java.exe、java.exe，后两个 java.exe 进程的路径应为 iMC 安装目录。

（c）1812、1813 对应的 IP 应为 UAM 服务器实际 IP 地址、50200、9019 对应的 IP 应为 iMC 服务器实际的 IP 地址或者 0.0.0.0。

（3）iMC 服务器和接入设备可达性检查

单击“业务”→“用户接入管理”→“接入设备管理”→“接入设备配置”命令后需添加接入设备发给 iMC 服务器 Radius 协议报文的端口 IP，iMC 默认会同该 IP 进行 Radius 协议报文交互，需保证 iMC 可以 ping 通该 IP，本例中接入设备 IP 应为 172.16.100.1，如图 8-322 所示。



图 8-322　iMC 服务器和接入设备可达性检查

说明：接入设备会有多个 IP 地址，如果要更改接入设备 IP，需在 Radius Scheme 视图下配置如下命令。

[sw-radius-h3c] nas-ip 172.16.2.1，并在 iMC 上更改为 172.16.2.1。

（4）设备侧配置检查

如果是 802.1x 认证，则需进行如下配置。

```
[BAS-radius-h3c]display this
# Radius 方案配置
radius schemeh3c
server-type extended
primary authentication 172.16.100.122
primary accounting 172.16.100.122
key authenticationh3c
key accountingh3c
nas-ip 172.16.100.1
```

```
[BAS-isp-dot1x]display this
#域配置
domaindot1x
 authenticationlan-access radius-scheme h3c
 authorizationlan-access radius-scheme h3c
 accountinglan-access radius-scheme h3c
[sw]dot1x
[sw]dot1x authentication-method eap
[sw-GigabitEthernet1/0/12]dot1x
```

说明：

① H3C 设备默认的认证方式为 CHAP，证书认证必须为 EAP 方式(透传证书信息)，所以必须将认证方式改为 EAP。

② Radius nas-ip 默认为与 iMC 服务器相连接口的 IP 地址。

如果是 Portal 认证，则需在设备上进行如下配置。

```
# Radius 方案配置
radius schemeh3c
server-type extended
primary authentication 172.16.100.122
primary accounting 172.16.100.122
key authenticationh3c
key accountingh3c
nas-ip 172.16.100.1
---------------------------------------------
# 域配置
domainportal
authenticationportal radius-scheme h3c
authorizationportal radius-scheme h3c
accountingportal radius-scheme h3c
---------------------------------------------
portal 配置
[sw]portal server portal ip 172.16.100.122 key h3c url http://172.16.100.122:8080/portal
[sw-Vlan-interface1]ip add 172.16.16.1 24
[sw-Vlan-interface1]portal server portal method direct
[sw-Vlan-interface1] portal nas-ip 172.16.16.1
```

(5) UAM 接入设备配置检查

① 共享密钥须和接入设备配置保持一致。

② 接入设备类型：根据实际情况选择。

③ 组网方式：如果接入设备支持计费报文，则选择不启用混合组网，如果接入设备不支持计费报文，则选择启用混合组网。

④ 设备 IP：默认是发给 iMC 服务器 Radius 报文的接口 IP 地址，本例中应为 172.16.100.1，如图 8-323 所示。



图 8-323 UAM 接入设备配置检查

说明： 如果填写接入设备其他端口 IP 作为接入设备 IP，须在 Radius Scheme 视图下配置 nas-ip：192.168.2.1。

（6）UAM 服务配置检查

检查 UAM 接入服务中的服务后缀是否和接入设备的 Domain、Radius Scheme 配置保持一致；确认该接入规则是否配置了正确的认证方式(是 TLS 还是 PEAP 方式)，如图 8-324 所示。对于 EAP 认证模式，iNode 客户端(手机自带客户端)后缀是否添加、认证设备 Domain 配置、iMC 上的服务后缀配置对应关系可参考表 8-5。



图 8-324　默认接入规则

表 8-5　后缀配置关系

iNode 认证连接用户名	设备用于认证的 Domain	设备配置相关命令	iMC 中服务后缀
X@Y	Y	With-domain	Y
		Without-domain	Y
X	Default Domain	With-domain	无后缀
		Without-domain	无后缀

在“证书认证类型”里面确认勾选的是 TLS 还是 PEAP 认证方式，如图 8-325 所示。



图 8-325　证书认证类型

说明：EAP 认证方式会透传所有报文，此时设备侧配置的 user-name-format 作用失效，客户端认证用户名如果包含后缀，则服务里面也必须有后缀，如果客户端认证用户名不带后缀，则服务里面也一定不要带后缀。

（7）UAM侧证书配置检查

证书配置路径为："用户"→"接入策略管理"→"业务参数配置"→"证书配置"→"查看配置信息"，如果是证书认证，则iMC侧必须有根证书和服务器证书，确认证书仍在有效期内且保证从根证书到服务器证书的证书链完整。iMC支持的根证书文件格式为：pem(base64位编码，文件后缀为.pem或.cer)，der(der编码，文件后缀为.der或.cer)，pkcs12(pkcs12编码，文件后缀为.pfx或.p12)。注意：如果证书格式是pfx格式，则不支持pvk格式的私钥文件。iMC支持的服务器证书文件格式为：pem(base64位编码，文件后缀为.pem或.cer)，der(der编码，文件后缀为.der或.cer)，pkcs12(pkcs12编码，文件后缀为.pfx或.p12)；若服务器证书和私钥在同一个文件，则不能使用der文件，如图8-326所示。



图8-326　UAM侧证书配置检查

（8）是否Portal认证

如果是Portal认证则转向UAM Portal配置检查，如果是802.1x认证，则直接确认是否LDAP+EAP+MSCHAPV2认证。

（9）UAM Portal配置检查

Portal有服务类型配置，如果需要配置服务类型，需保证服务类型标示和域名保持一致，服务类型无要求，可随便写一个好记的名称，如图8-327所示。



图8-327　服务类型

保证用户认证的IP地址已经添加到IP地址组里面，如图8-328所示。

确认已配置Portal设备如图8-329所示。



图 8-328　IP 地址添加



图 8-329　确认已配置 Portal 设备

说明：

① IP 地址：默认为启用 Portal 认证 vlan 接口的 IP 地址，本例中即为 172.16.16.1，也可以修改为设备上其他接口地址，单需要在 vlan 接口视图下配置：Portal nas-ip x. x. x. x。

② 端口默认为 2000，无须修改。

③ 密钥：和 portal server portal keyxxx url http://ip:port/portal 中 xxx 保持一致。

④ 组网方式：终端和认证 vlan 属同一网段时选择直连，不在同一网段时选择三层。

最后再确认该 Portal 设备下的端口组已经正确关联到用户的 IP 地址段，如图 8-330 所示。



图 8-330　Portal 设备下的端口组

说明：

① 认证方式：证书认证必须选择为 EAP 认证。

② IP 地址组：确认关联的是用户的 IP 地址段。

(10) 是否 AD 用户+PEAP+MS-CHAPV2 证书认证

确认认证用户是否属于 AD 认证用户，是否采用 PEAP MS-CHAPV2 证书认证，确认方式如下，如果不属于此种情况，则直接检查 UAM 账号配置，如图 8-331 所示。



图 8-331　证书认证确认

说明： AD 用户：仅指从微软 LDAP 服务器同步过来的用户，open LDAP 用户无须配置 PEAP 预控服务器；iMC 仅同步用户账户，并不同步用户密码。

(11) 域控服务器侧虚拟计算机配置检查

① 虚拟计算机名称和路径检查。虚拟计算机必须在 Computers 下新建，首先保证虚拟计算机路径正确，路径格式一般为 CN=ComputerName，CN=Computers，DC=XXX，DC=XXX，本例中路径的正确写法为：CN=H3C，CN=Computers，DC=H3C，DC=Com；然后需保证该名称和“UAM 侧域控服务器配置检查”配置的虚拟计算机名称保持一致，如图 8-332 所示。



图 8-332　与虚拟计算机名称一致

② 虚拟计算机密码检查。虚拟计算机密码检查分为以下 3 个步骤。

第 1 步，从 UAM 服务器下载密码修改脚本，如图 8-333 所示。



图 8-333　修改脚本

第 2 步，确认密码修改脚本的内容，该密码需和“UAM 侧域控服务器配置”设置的虚拟计算机密码保持一致，如图 8-334 所示。

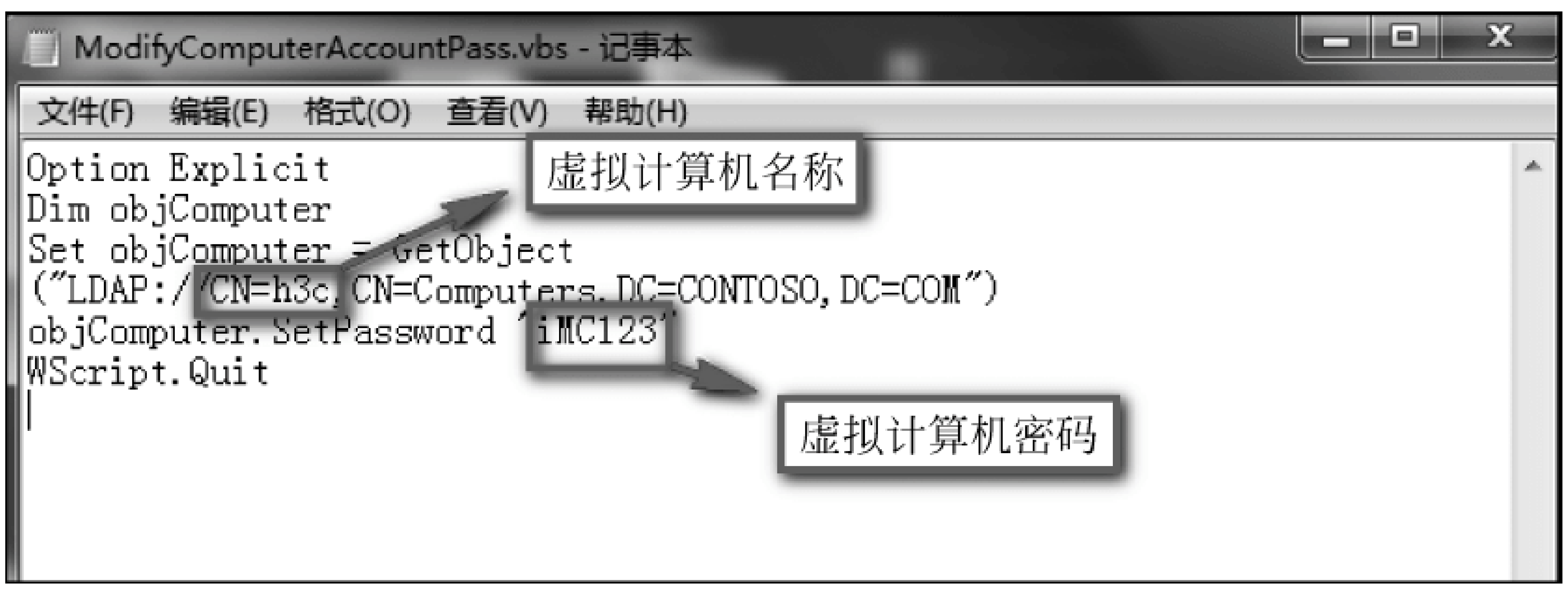


图 8-334　与虚拟计算机密码一致

第 3 步，在域控服务器侧 CMD 下使虚拟计算机密码生效。

确认密码和名称无误后，在域控服务器 CMD 命令行下执行该脚本，执行后不能有出错提示，如果不能保证之前是否正确执行，可再次执行该脚本，如图 8-335 所示。



图 8-335　在 CMD 命令下执行脚本

（12）UAM 侧域控服务器配置检查

域控服务器全名是指 AD 服务器的计算机名称，虚拟计算机名称和密码需和“域控服务器即配置”侧的配置保持一致，如图 8-336 所示。



图 8-336　PEAP 认证域控配置

说明：

① DNS 服务器 IP：必须填写实际 IP 地址，不能填写 127.0.0.1。

② 域控服务器 IP：必须填写实际 IP 地址，不能填写 127.0.0.1。

③ 本地服务器端口：确认不要修改此端口号。

④ 域控服务器操作系统版本：如果使用 iNode 客户端认证，则此处填写实际操作系统版本，其他情况均填写 Windows 2003 或之前版本。

虚拟计算机全名的查看方法如图 8-337 所示。



图 8-337　虚拟计算机全名查看

(13) UAM 账号信息检查

确认账号状态、绑定信息、引用的服务，并根据配置对引用的服务进行检查，如图 8-338 所示。



图 8-338　UAM 账号信息检查

说明：该步骤主要是确认账号引用的服务，该服务中是否引用了之前配置的接入策略。

(14) iNode 客户端配置检查

证书认证＋802.1x，可以使用系统自带客户端；证书认证＋Portal 必须使用 iNode；客户端证书配置分以下两种情况。

① EAP-TLS 证书认证。

EAP-TLS 证书认证时，客户端必须安装客户端证书，默认客户端证书名称必须和接入账户名保持一致，否则会提示证书无效，如图 8-339 所示。

如果客户端没有根证书则不能选择“验证服务器证书”单选框。

② EAP-PEAP 证书认证。

采用 PEAP 证书认证时，客户端可以没有任何证书；客户端没有根证书时，则不能选择“验证服务器证书”单选框，如图 8-340 所示。



图 8-339 验证服务器证书

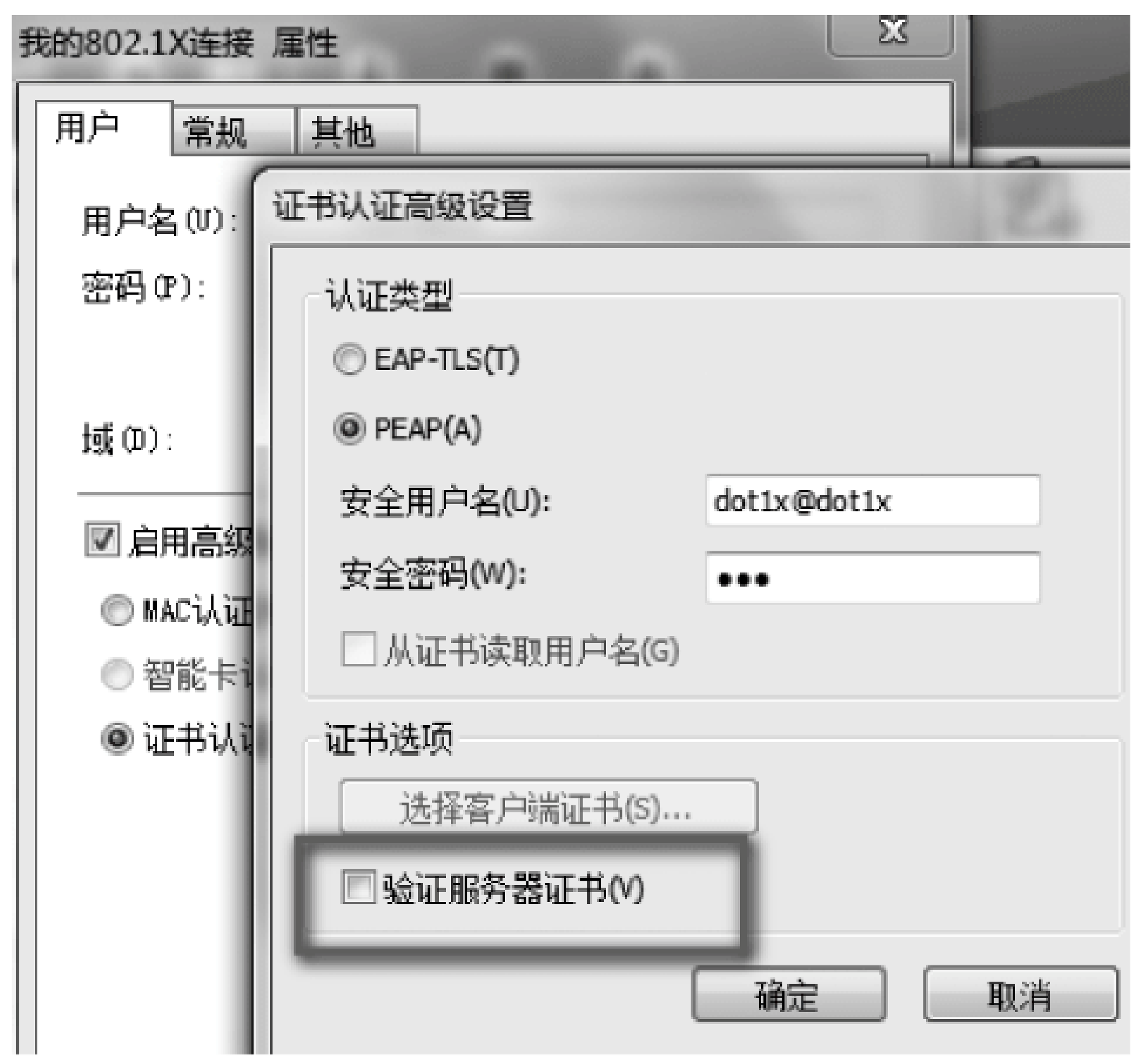


图 8-340 选择验证服务器证书

说明：

(a) EAP-TLS：双向证书认证，客户端必须有客户端证书，如果不验证服务器证书，客户端可以没有根证书。

(b) PEAP：单向证书认证，客户端可以没有认证证书。

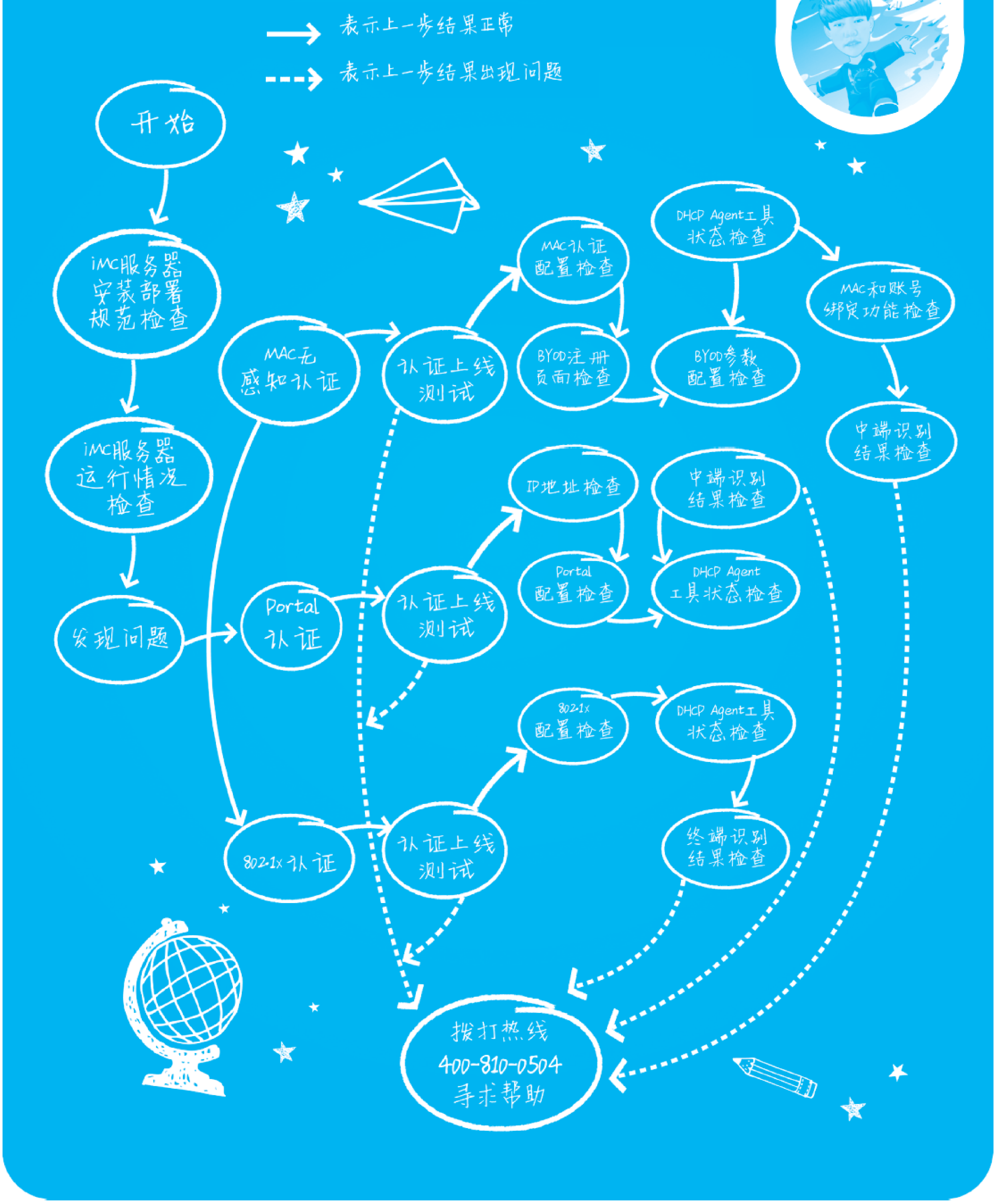
(15) iNode 客户端账号信息检查

iNode 客户端账号及后缀配置请参考表 8-6。

表 8-6 iNode 客户端账号及后缀配置

iNode 认证连接用户名	设备用于认证的 Domain	设备配置相关命令	iMC 中服务后缀
X@Y	Y	With-domain	Y
		Without-domain	Y
X	Default Domain	With-domain	无后缀
		Without-domain	无后缀

EIA之BYOD特性故障排查



1. 开始

当前，移动互联网在全球掀起了新的发展高潮，特别是随着移动智能终端的日益普及，移动应用和服务不断丰富，迅速进入了移动互联网高速发展阶段。特别是移动互联网用户数量、终端数量、市场规模的增长速度和态势非常迅猛，移动互联网蕴含着巨大的市场空间和发展前景。智能手机，平板电脑等移动终端彻底改变了人们的生活方式，不管对于企业，还是个人，自由选择办公终端无疑可以提高工作效率，所有的这些，都促生了 BYOD（Bring Your Own Device）的产生和繁荣。BYOD 指带自己的终端上班，这些设备包括个人电脑、手机、平板等，现在更多情况指手机或平板这样的移动智能终端设备，目前 BYOD 技术主要集中在如何解决移动终端（手机、平板、POS 机等）认证控制的方案，主要解决：①终端的智能识别。②基于用户身份和终端类型的认证和权限控制。③基于终端和身份的安全控制，简而言之，即同一个账号用不同的终端上线下发不同的网络访问权限以确保内网的安全。

BYOD 排错的基本思路：BYOD 是一种新型的解决方案，其中最重要的技术关键是终端识别，H3C EIA 当前支持 DHCP 特征识别、HTTP User Agent 特征识别、MAC 地址识别、iNode 客户端识别 4 种方式来识别终端的厂商、终端类型、操作系统等信息，可以基于不同的认证方式，包括 MAC 认证、Portal 认证、802.1x 认证来实现，而在不同的认证方式场景，可以选择不同的终端识别技术。既然 BYOD 基于准入控制，那么首先检查服务器软硬件及性能是否满足当前认证需要，然后根据不同的认证方式进行检查。

2. 流程图相关操作说明

（1）iMC 服务器安装部署规范检查

需要对照《智能管理中心（iMC）部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心（iMC）部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心（iMC）部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心（iMC）部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“EIA”“EIP（终端智能识别）功能模块”是否已经部署，如图 8-341 所示。

说明： EIA V7 版本开始，BYOD 功能需要购买 EIP 授权才能使用。EIP（终端智能识别）属于 EIA 的一个功能模块，如果需要部署 BYOD，必须部署 EIP 模块。

（2）iMC 服务器运行情况检查

要顺利实施 BYOD 解决方案，除了确保 UAM 相关进程运行正常外，还要检查策略服务器对应的进程及绑定的端口是否正常，具体检查方式请参考认证类和 EAD 管理云图，此外，必须确保 BYOD 的 EIP 功能模块后台对应的 eipserver 进程运行正常，如下所示。

单击“开始”→“智能部署监控代理”命令，选择“进程”标签，查看 EIP 的进程 eipserver 是否正常启动，具体如图 8-342 所示。



图 8-341 部署情况

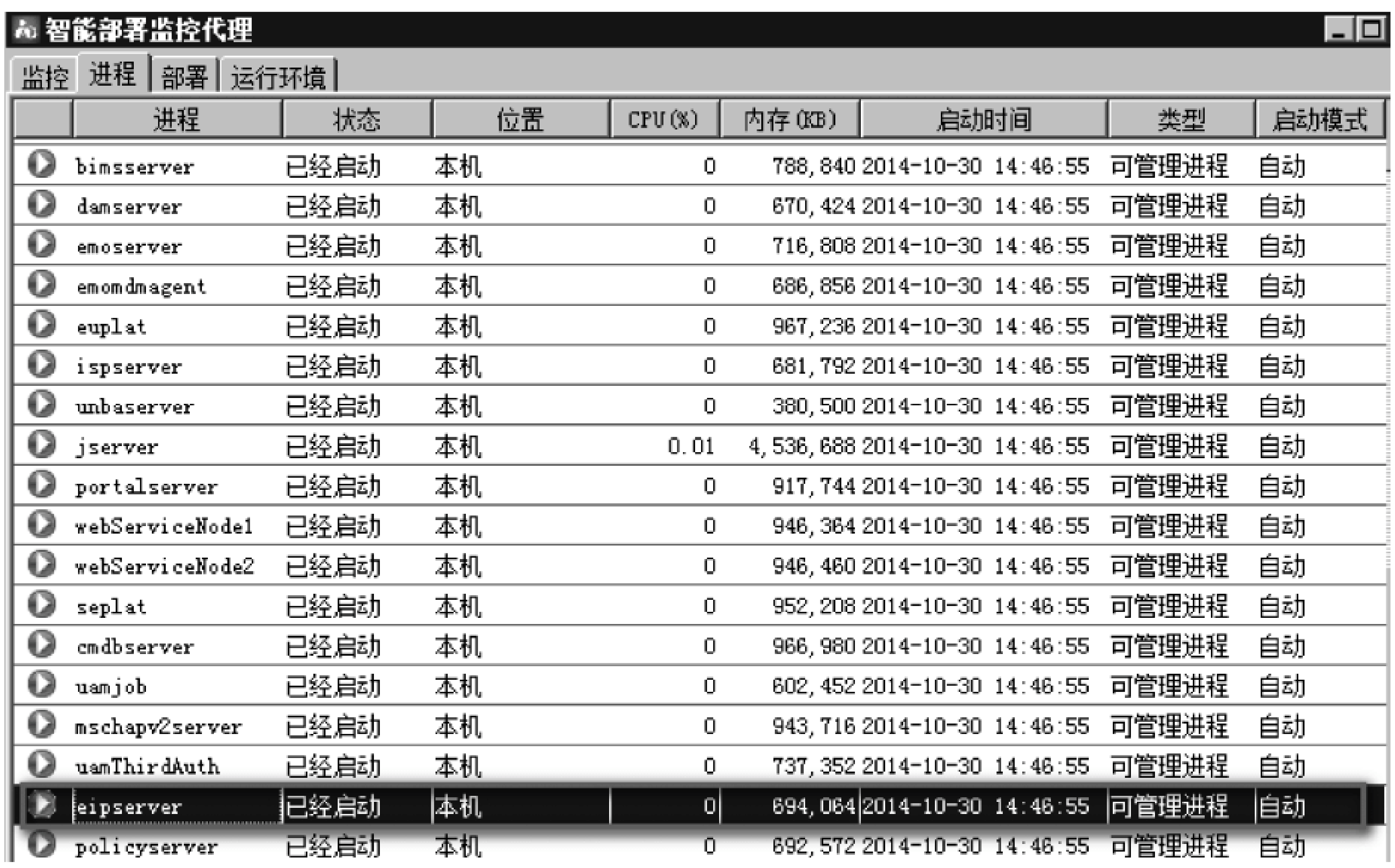


图 8-342 进程启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(3) MAC 无感知认证实现 BYOD 的配置检查

为了实现所有终端完全无感知快速接入网络，EIA 侧提供了 BYOD 匿名账号的快速认证，即认证设备侧启用 MAC 认证，EIA 服务器侧创建 byodanonymous 账号，所有终端接入网络即可快速以终端 MAC 地址作为登录名，byodanonymous 为接入用户通过认证，为了适当分配授权，为 byodanonmous 账号创建了单独的服务，也可灵活地通过 BYOD 注册页面将当前 MAC 地址和正式账号或访客账号进行绑定来实现授权的快速变更，既快捷又方便。在 MAC 无感知认证实现 BYOD 场景需要从如下几方面进行排查。

① MAC 认证配置检查。MAC 无感知认证基于 MAC 认证，而实现 BYOD 的前提是 MAC 认证正常，有关 MAC 地址认证的配置方法请参考认证类相关云图或相关产品配置手册，在此不再叙述。

② BYOD 注册页面配置检查。用户可以通过 EIA V7 的“终端页面定制”功能自行定制 BYOD 注册页面，如图 8-343 所示。



图 8-343　BYOD 注册页面

在定制完毕 BYOD 注册页面后，需要重启 iMC 相关进程（集中式部署时重启 jserver，EIP 部署在从机上时重启 webserver）才会生效。

③ BYOD 参数配置检查。

(a) 首选需要创建 byodanonymous 账号，单击“用户”→“接入用户”→“增加接入用户”命令，增加或选择一个已经存在的用户姓名后，选择“默认 BYOD 用户”选项框即可自动生成 byodanonymous 账号，如图 8-344 所示。



图 8-344　创建账号

(b) 启用 MAC 无感知认证，单击“用户”→“接入策略管理”→“业务参数配置”→“系统配置”→“终端管理参数配置”命令，选择“启用 MAC 无感知认证”为“是”，如图 8-345 所示。

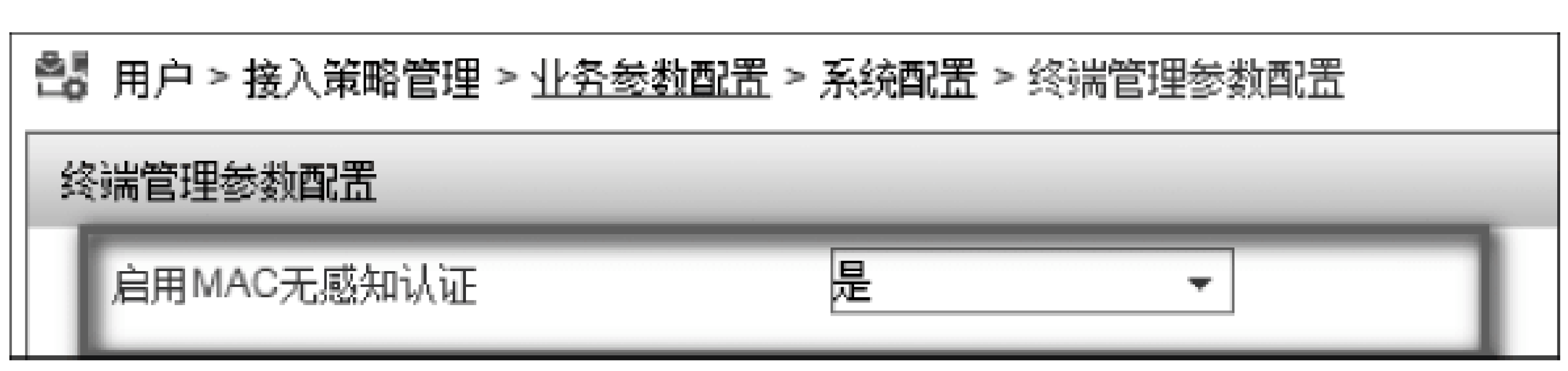


图 8-345　启用 MAC 无感知认证

说明：此处如果不选择“是”启用 MAC 无感知认证，那么 MAC 认证可以通过，但是不能实现 MAC 和账号来进行授权的变更。

(4) H3C DHCP Agent 工具状态检查

MAC 无感知认证需要 DHCP 指纹法来进行终端识别，需要在 DHCP 服务器侧安装 H3C

DHCP Agent 工具,由该工具监控 DHCP 服务器的地址分发过程,并截获终端发送的 DHCP 请求报文中的 Option55 字段给 EIA 服务器,如图 8-346 所示。

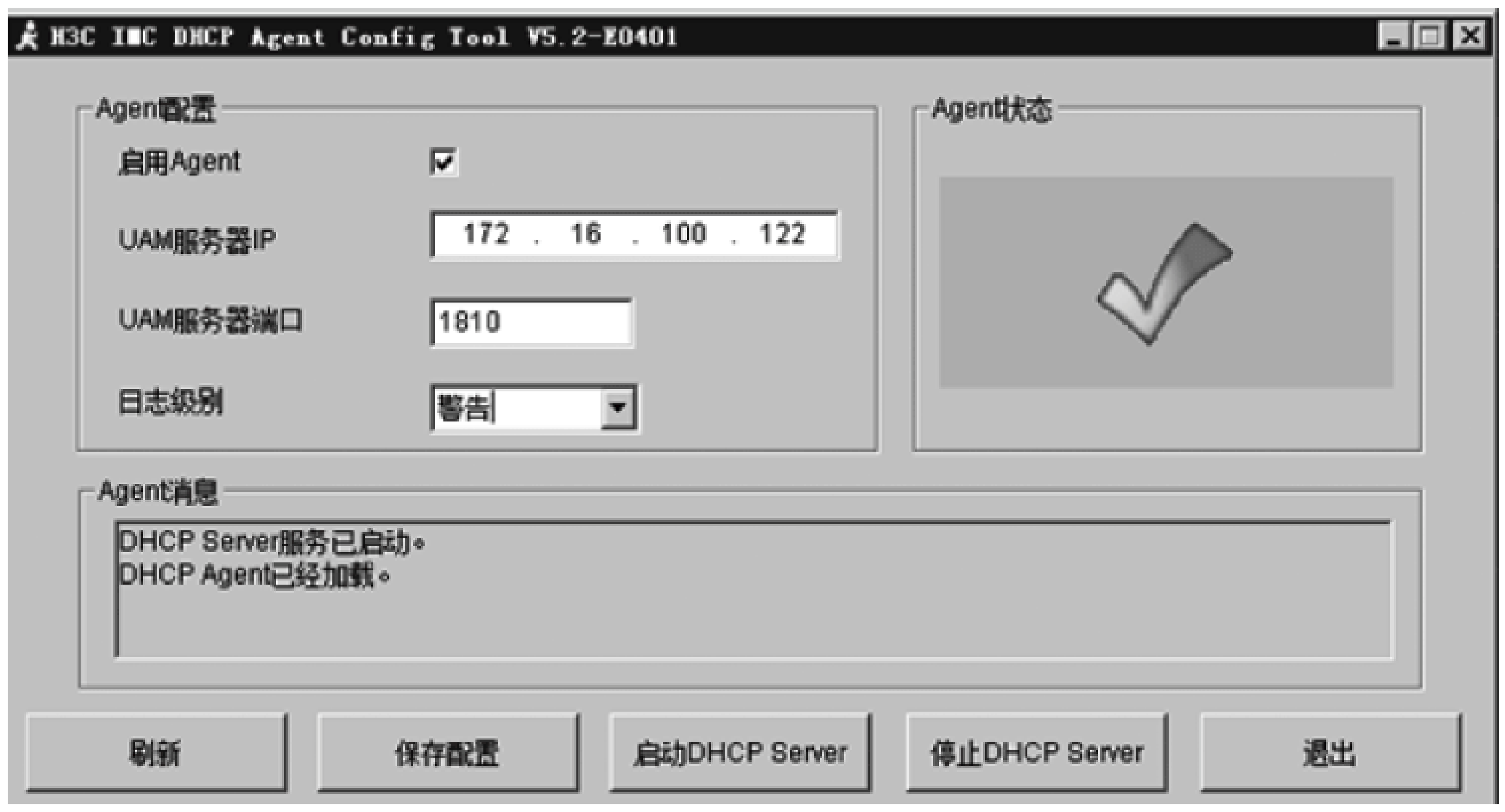


图 8-346　H3C DHCP Agent 工具状态

说明:

① DHCP Agent 安装包见 EIA 安装包内,DHCP Agent 的版本需要和相应的 EIA 版本一一对应。

② "启用 Agent":即启动该 Agent 工具。

③ "UAM 服务器 IP":即 UAM 部署的服务器 IP,如果 UAM 分布式部署,则填写分布式服务器 IP。

④ "UAM 服务器断开":UAM 服务器监听报文的端口,不建议修改。

⑤ "日志级别":分为"致命/错误/警告/信息/调试"5 个级别,默认"警告"级别,在问题定位时需要收集调试级别日志。

⑥ 修改配置后,需要单击"保持配置",并"启动 DHCP Server"。

(5) MAC 地址和账号绑定检查

匿名 MAC 认证成功后,如果需要做权限变更,就涉及通过 BYOD 注册页面将当前 MAC 地址和正式账号或访客账号进行绑定,绑定完毕后,策略服务器会踢用户下线,重新认证上线,此时认证方式还是 MAC,但是拥有之前绑定账号或访客服务的权限,如图 8-347 所示。



图 8-347　MAC 地址绑定正式账号前查看账号名

① MAC 地址绑定正式账号前查看账号名。单击"用户"→"终端设备管理"命令,其账户名为 byodanonymous。

② MAC 绑定正式账号后，其账号名变更为 byod，如图 8-348 所示。



图 8-348 账号名变更

(6) 终端识别结果检查

在用户认证成功后，根据管理员配置的不同接入场景而下发不同控制策略来进行授权，举例：管理员创建了一个服务：111，该服务里绑定了两个接入场景，分别对应 Windows 和 Andriod 操作系统，并分别下发不同的接入策略，如图 8-349 所示。即 Windows 终端上线后下发接入策略“123456”，Andriod 终端上线后下发接入策略“access permit”。



图 8-349 不同接入场景

说明：一个服务可以绑定多个接入场景，不同的接入场景可以根据不同的接入条件下发不同的接入策略来进行授权分发。

当一个终端认证通过后，可以单击“用户”→“终端设备管理”命令，在如图 8-350 所示页面查看该终端对应的终端类型、操作系统、厂商等信息。

(7) Portal 认证实现 BYOD 的配置检查

Portal 认证，Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。基本思想：未认证用户上网时，认证设备会强制用户登录到特定 Web 站点，用户可以免费访问该 Web 站点的服务。当用户需要使用互联网中的其他信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。Portal 业务可以为客户提供方便的管理功能，门户网站可以开展广告、社区服务等个性化业务，为了方便客户对

门户网站的个性化定制，EIA V7 版本开始还增加了终端页面定制功能，针对 PC 和 Phone 两种终端类型提供了大量的 Portal 登录页面、认证成功页面、心跳页面的模板，用户可以便捷地定制出适合自己的 Portal 页面，然后根据不同的 AP、不同 IP 地址段、不同操作系统推送不同的 Portal 页面。Portal 认证场景可以使用 iNode 客户端，也可以使用浏览器免客户端进行认证，由于三层协议架构使得 Portal 认证在组网上非常灵活，正因为如此，Portal 认证场景下的 BYOD 也深受客户喜爱。



图 8-350 终端类型页面

Portal 认证方式下实施 BYOD，主要针对客户公司内部员工或外来访客。

公司内部员工都有自己的认证上网账号，而外来访客可以通过用户自助或短信方式进行开户。终端在认证前必须获得 IP，所以 DHCP 指纹识别法常用于 Portal 认证场景的 BYOD，一般排查步骤如下。

① 终端 DHCP 是否获取到了正确的 IP。直接打开网卡属性查看或打开终端 PC 的 CMD 命令行窗口输入 ipconfig /all，回车如图 8-351 所示。如果是手机终端，则直接检查无线网络是否获取到了 IP。

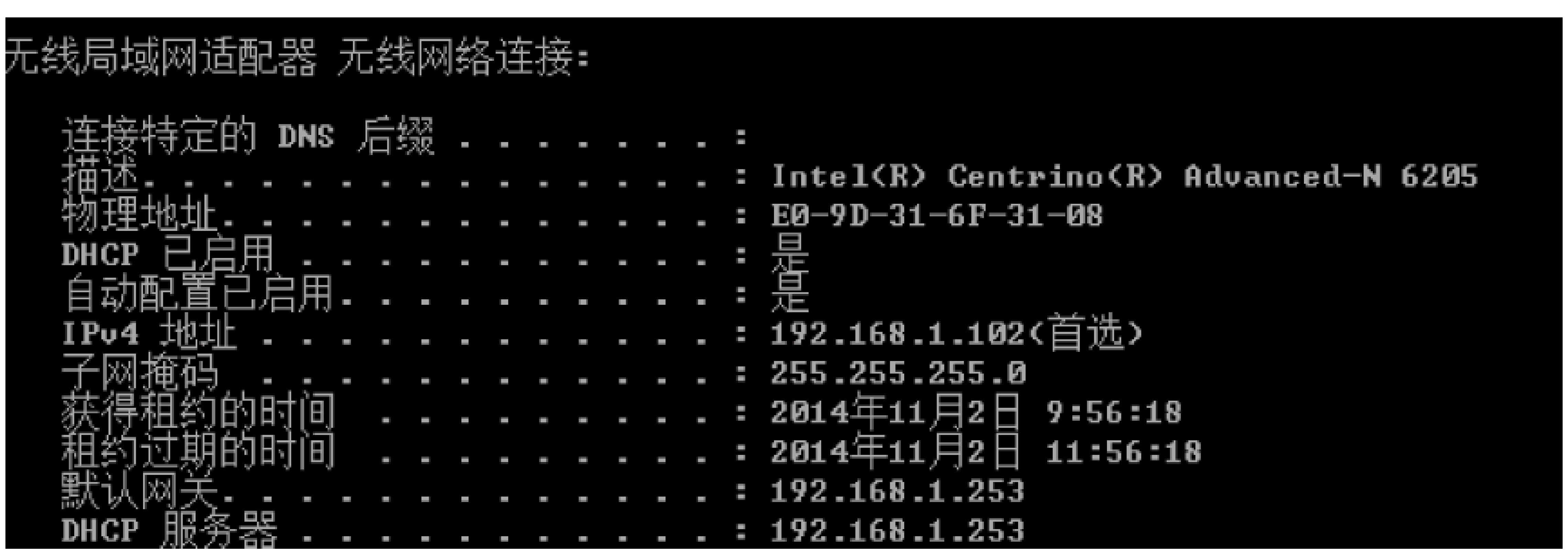


图 8-351 确认 DHCP 是否获取正确 IP

② Portal 配置检查。BYOD 的前提是确保 Portal 认证正常，有关 Portal 认证的配置方法，请参考 Portal 认证排查云图或公司官网的典型配置手册，本文不再详细叙述。

③ H3C DHCP Agent 工具状态检查。如果采用 DHCP 指纹法来进行终端识别，需要在 DHCP 服务器侧安装 H3C DHCP Agent 工具，由该工具监控 DHCP 服务器的地址分发过程，并截获终端发送的 DHCP 请求报文中的 Option55 字段给 EIA 服务器，如图 8-352 所示。

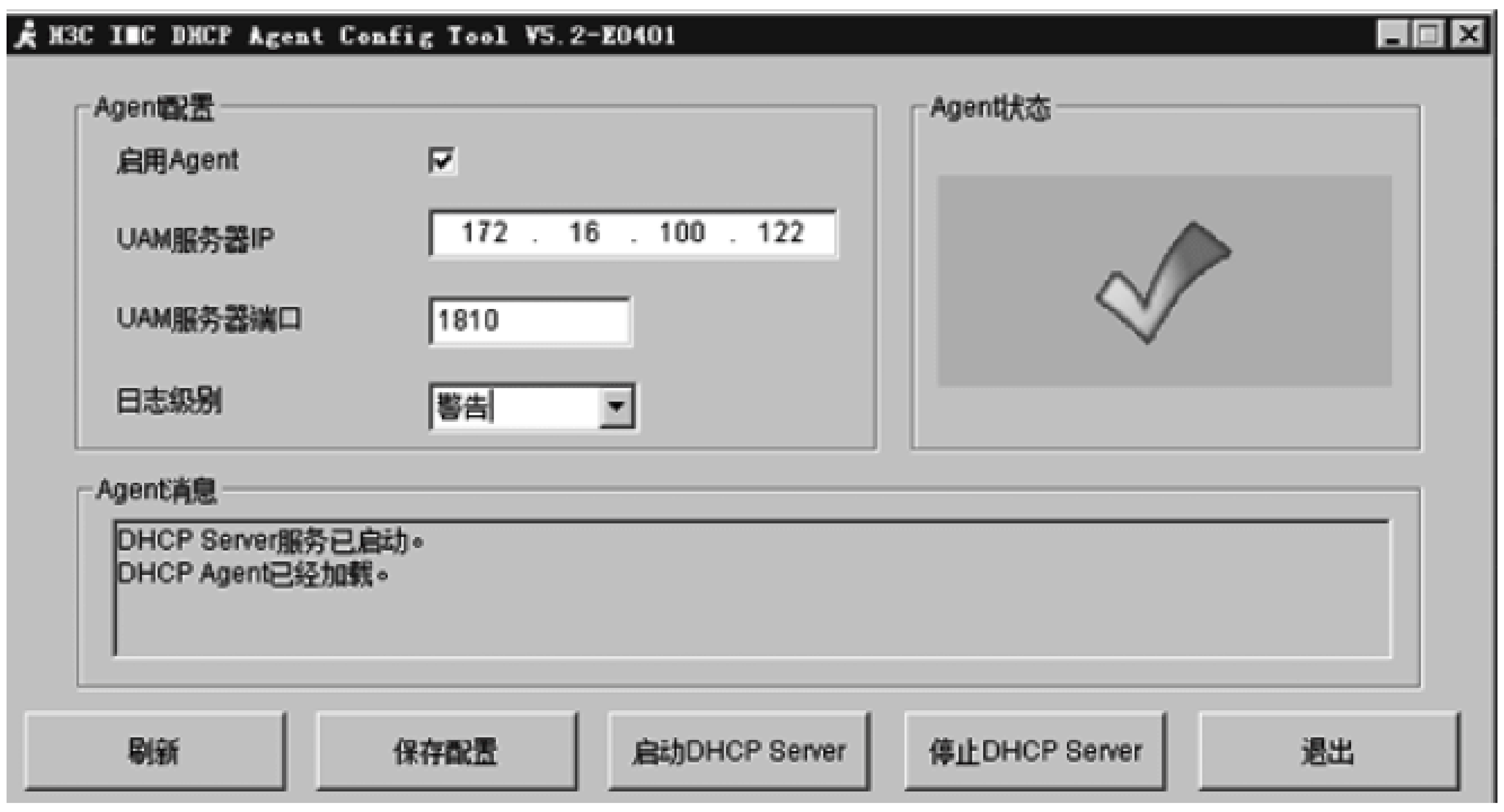


图 8-352　H3C DHCP Agent 工具状态检查

说明：

(a) DHCP Agent 安装包见 EIA 安装包内，DHCP Agent 的版本需要和相应的 EIA 版本一一对应。

(b)“启用 Agent”：即启动该 Agent 工具。

(c)“UAM 服务器 IP”：即 UAM 部署的服务器 IP，如果 UAM 分布式部署，则填写分布式服务器 IP。

(d)“UAM 服务器断开”：UAM 服务器监听报文的端口，不建议修改。

(e)“日志级别”：分为“致命/错误/警告/信息/调试”5 个级别，默认“警告”级别，在问题定位时需要收集调试级别日志。

(f) 修改配置后，需要单击“保持配置”，并“启动 DHCP Server”。

④ 终端识别结果检查。

在用户认证成功后，根据管理员配置的不同接入场景而下发不同控制策略来进行授权，举例：管理员创建了一个服务：111，该服务里绑定了两个接入场景，分别对应 Windows 和 Andriod 操作系统，并分别下发不同的接入策略。即 Windows 终端上线后下发接入策略“123456”，Andriod 终端上线后下发接入策略“access permit”，如图 8-353 所示。



图 8-353　不同接入场景

说明：一个服务可以绑定多个接入场景，不同的接入场景可以根据不同的接入条件下发不同的接入策略来进行授权分发。

当一个终端认证通过后，可以单击“用户”→“终端设备管理”命令，在如图 8-354 所示页面查看该终端对应的终端类型、操作系统、厂商等信息。



图 8-354　页面查看

⑤ 802.1x 认证实现 BYOD 的配置检查。

(a) 802.1x 的配置检查。

802.1x 配置检查包括 iMC 服务器侧的配置包括接入设备、服务、接入策略等配置以及认证设备侧配置，具体的配置方法请参考 802.1x 认证排查云图，本文不再详细叙述。

(b) H3C DHCP Agent 工具状态检查。

如果采用 DHCP 指纹法来进行终端识别，需要在 DHCP 服务器侧安装 H3C DHCP Agent 工具，由该工具监控 DHCP 服务器的地址分发过程，并截获终端发送的 DHCP 请求报文中的 Option55 字段给 EIA 服务器，如图 8-355 所示。



图 8-355　工具状态检查

说明：

ⓐ DHCP Agent 安装包见 EIA 安装包内，DHCP Agent 的版本需要和相应的 EIA 版本一一对应。

ⓑ “启用 Agent”：即启动该 Agent 工具。

ⓒ “UAM 服务器 IP”：即 UAM 部署的服务器 IP，如果 UAM 分布式部署，则填写分布式服务器 IP。

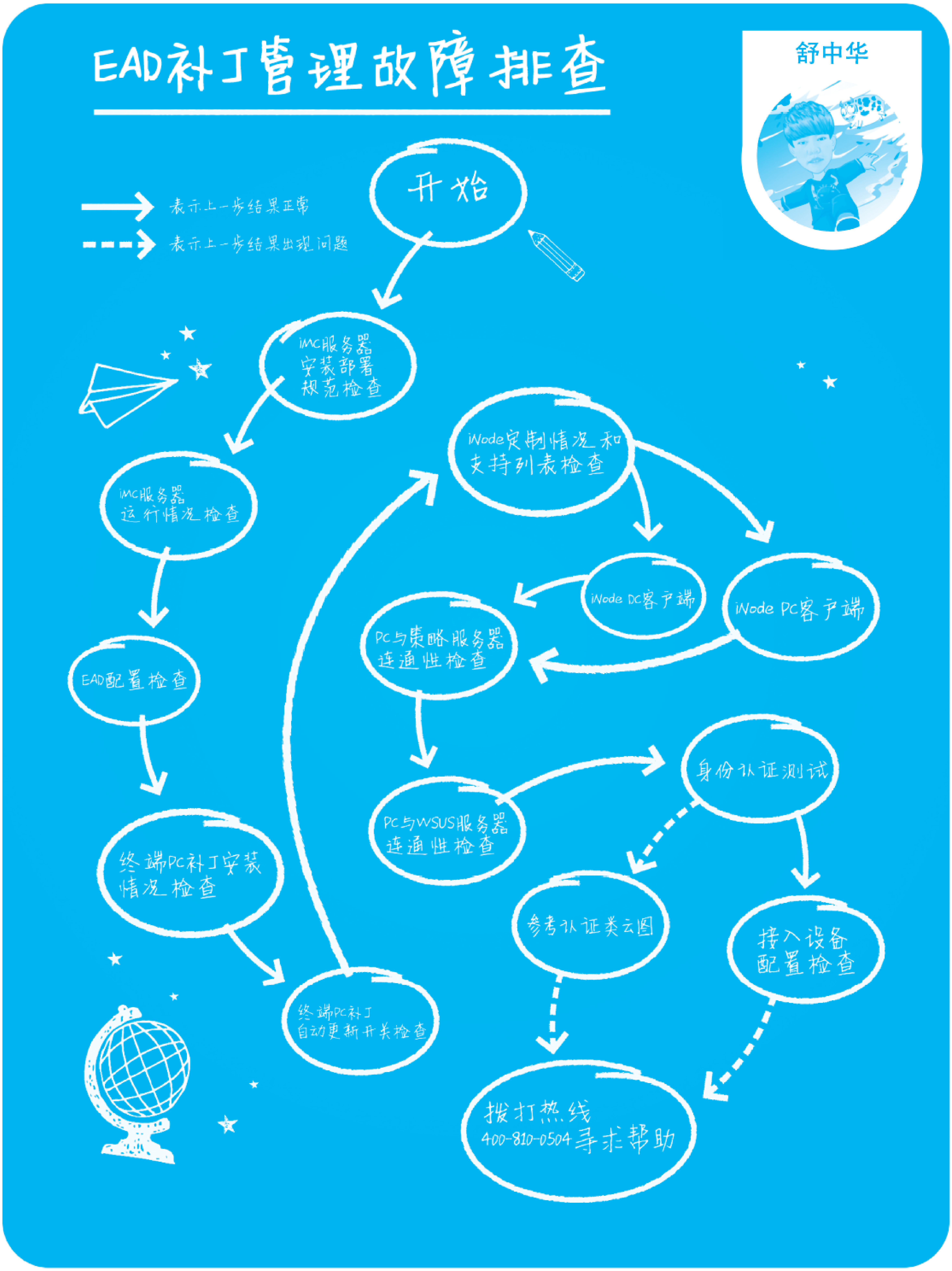
ⓓ“UAM 服务器断开”：UAM 服务器监听报文的端口，不建议修改。

ⓔ“日志级别”：分为“致命/错误/警告/信息/调试”5 个级别，默认“警告”级别，在问题定位时需要收集调试级别日志。

ⓕ 修改配置后，需要单击“保持配置”，并“启动 DHCP Server”。

(c) 终端识别结果检查。

802.1x 认证场景，一般是认证通过后再获取 IP，也就是说首次认证通过后 EIP 才识别该终端类型，所以第一次认证成功后该账户匹配的是默认接入策略，需下线重连才能匹配相关的接入策略下发相应的授权。


EAD补丁管理故障排查
舒中华
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
EAD配置检查
终端PC补丁安装情况检查
终端PC补丁自动更新开关检查
iNode定制情况和支持列表检查
iNode DC客户端
iNode PC客户端
PC与策略服务器连通性检查
PC与WSUS服务器连通性检查
身份认证测试
参考认证类云图
接入设备配置检查
拨打热线400-810-0504寻求帮助

1. 开始

EAD 补丁管理策略可以定期检查终端 PC 的补丁并结合补丁服务器自动更新补丁，将不符合策略要求的终端踢下线或限制在“隔离区”内，防止“危险”终端对网络安全的损害，避免“易感”终端受病毒、蠕虫的攻击。EAD 补丁管理排错思路：身份认证之后才会触发安全认证，关于身份认证失败的排查思路可以参考具体的认证类云图，在此不再叙述。

首先检查服务器软硬件及性能是否满足当前认证需要，然后从 iNode PC 和 iNode DC 两种客户端认证场景进行分析，相应做 iMC 服务器运行状态的检查，安全策略配置检查，终端补丁安装情况检查，补丁服务器运行状态检查，最后对终端 PC 和补丁服务器的连通性进行检查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“EAD 安全策略管理”各组件是否已部署的状态，具体如图 8-356 所示，关于“用户接入管理”组件的检查方式，请参考认证类云图。



图 8-356 组件部署状态

说明：EAD 安全策略管理—桌面资产管理和 EAD 安全策略管理—桌面资产管理代理服务器是桌面资产(DAM)管理的功能组件，在 EAD 解决方案中可以不部署。

(2) iMC 服务器运行情况检查

要顺利实施 EAD 解决方案，除了确保 UAM 相关进程运行正常外，还要检查策略服务器

对应的进程是否运行正常，及进程绑定的端口是否正常，具体可从如下两方面检查。

① 单击“开始”→“智能部署监控代理”命令，选择“进程”标签，查看 EAD 的核心进程 policyserver 是否正常启动，具体如图 8-357 所示。



图 8-357 进程启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

② 检查策略服务器对应的监听端口 UDP 9019，UDP 9017 是否正常绑定，如图 8-358 所示。

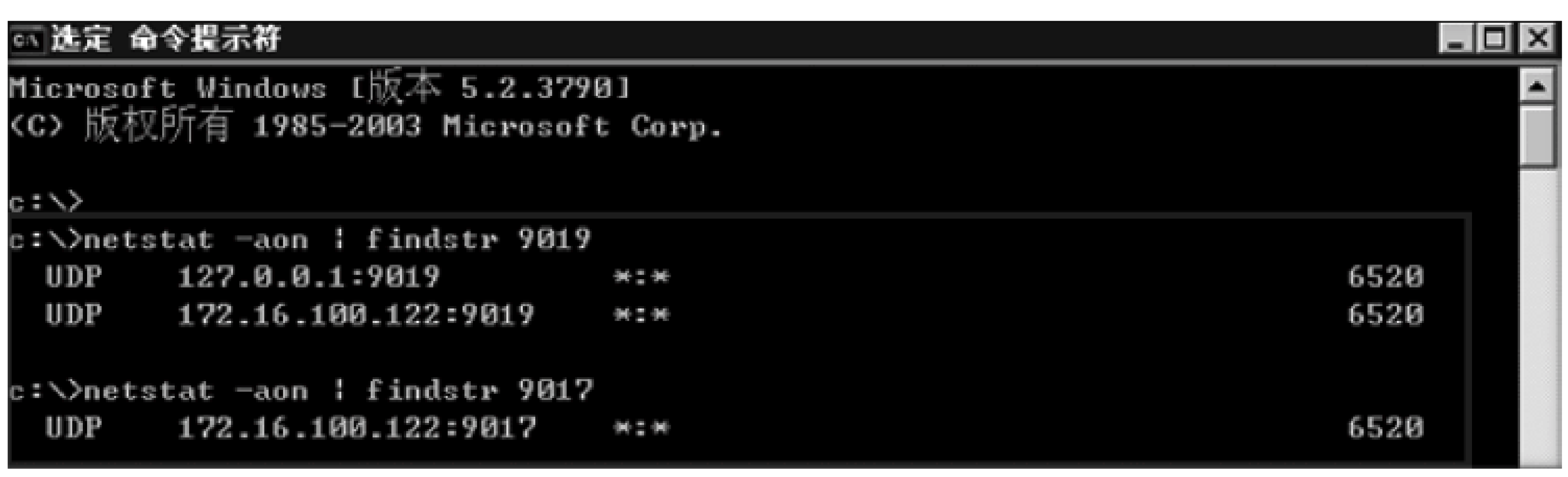


图 8-358 各端口正常绑定情况

说明 1：如图 8-358 所示，9019 端口号必须同时绑定两个 IP，分别是 127.0.0.1 和实际网卡 IP，如图 8-359 所示。172.16.100.122，而 9017 端口只需绑定实际网卡 IP 即可。

说明 2：Windows 操作系统中，通过命令 netstat -aon |findstr 端口号来显示某端口的监听状态以及对应的进程 PID，举例：对应提示符回显，如图 8-360 所示。

其中第一列 UDP 监听的协议；第二列 172.16.100.122：9017 所指监听的服务器的 IP 和端口号；第三列 *.* 代表监听状态；最后一列 6520 代表此协议监听的进程 PID，根据此 PID，对照 Windows 任务管理器，即可确定该端口绑定的具体服务。

(3) EAD 配置检查

要实施 EAD 的补丁管理，服务器侧必须创建安全策略，并且确保安全策略里配置了补丁检查方式以及隔离 ACL，VLAN 的配置，具体从如下两方面检查。

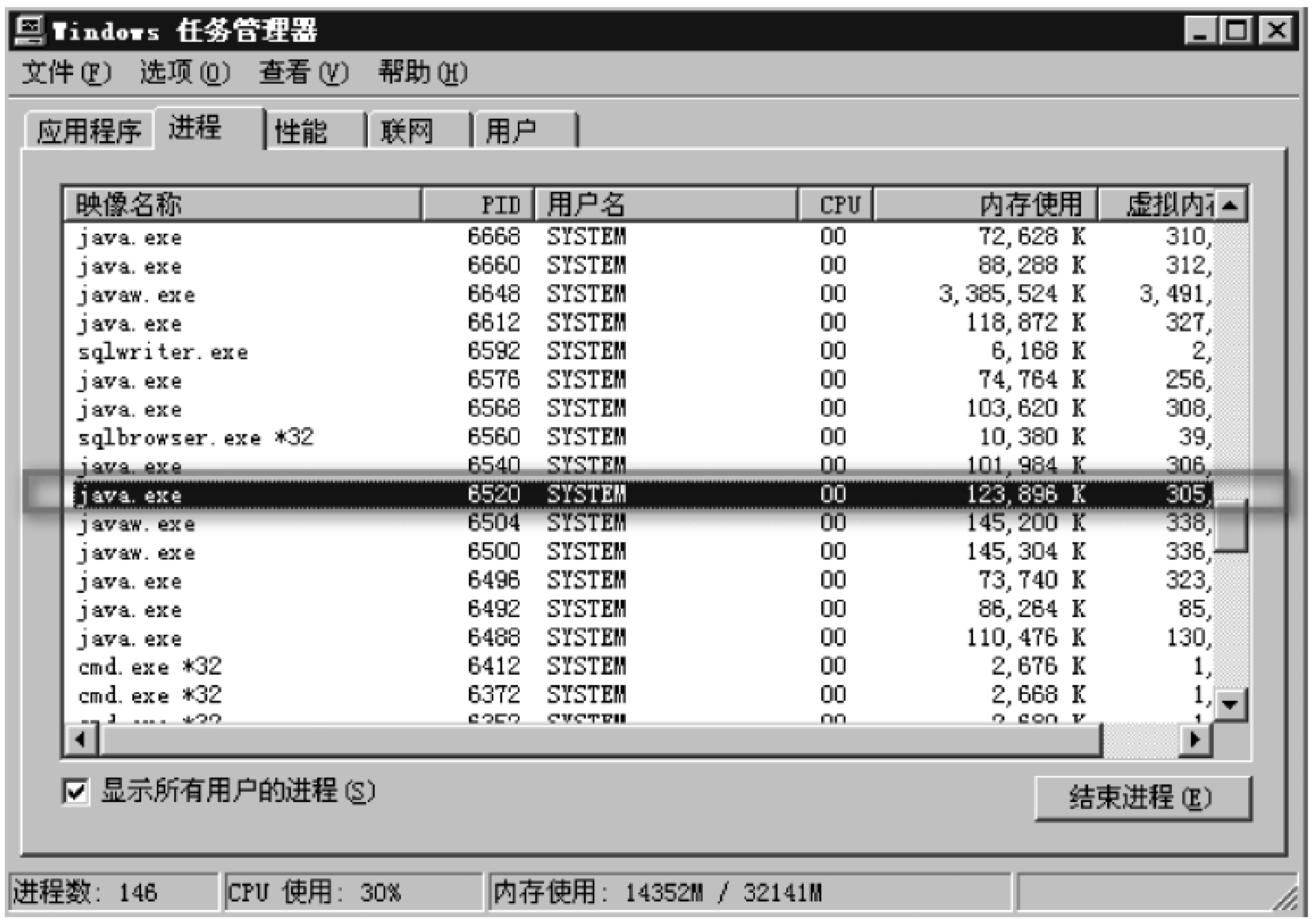


图 8-359　端口号绑定的 IP



图 8-360　提示符回显

① 排查补丁检查方式的配置。

只有账号绑定了正确的“服务”,“服务”绑定了正确的“安全策略”,“安全策略”配置了正确的“安全级别”和“补丁检查方式”,才会进行补丁的检查。

检查账号是否配置了正确的补丁检查方式最直观的方法。

通过接入账号确定其绑定的服务,然后通过服务确定其绑定的安全策略,通过安全策略确定具体的补丁检查方式和安全级别,安全级别是下线,隔离,提醒,还是监控,针对 Windows 系统支持手工检查和结合微软 WSUS 补丁服务器自动检查,具体如图 8-361 所示,单击“业务”→“EAD 安全软件”→“终端安全软件策略管理”命令。

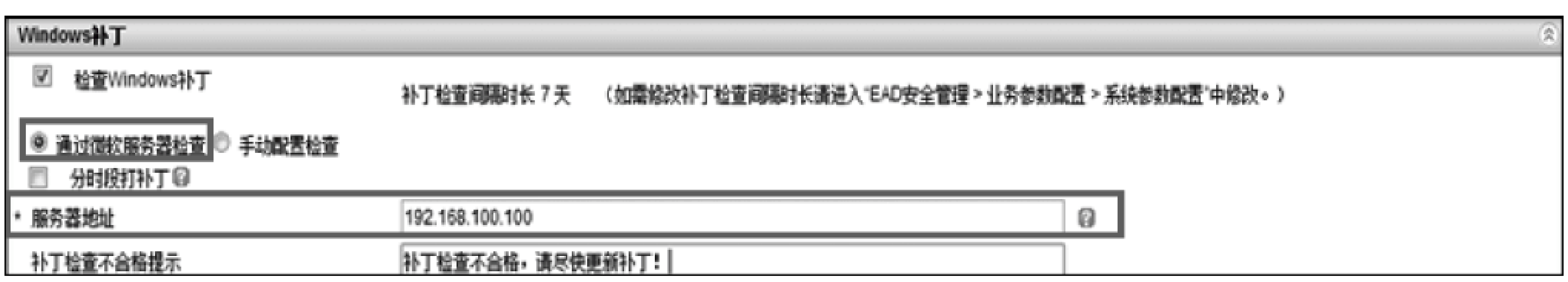


图 8-361　自动检查

如果需要通过微软服务器检查,则需要预先搭建 WSUS 补丁服务器(WSUS 补丁服务器的安装可参考 KMS - 6660),然后在图 8-361 的“服务器地址”栏中填写正确的补丁服务器 IP。

“补丁检查不合格提示”栏中填写的信息,在补丁检查不合格的时候会下发给 iNode 客户端提醒用户,如图 8-362 所示。

说明 1:

(a) EAD 手动检查补丁的方式,是根据 EAD 补丁管理中创建的补丁名称和补丁级别检查终端 PC 的补丁安装情况,然后在安全策略中的 Windows 补丁配置栏中选择“补丁级别”,

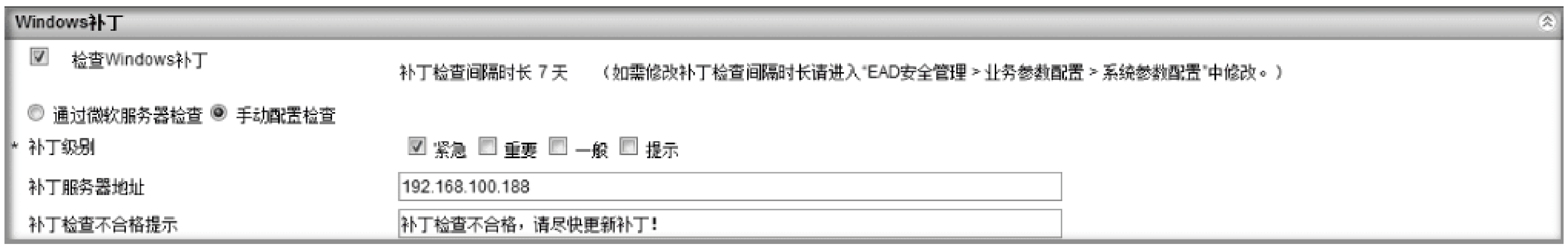


图 8-362　补丁检查不合格提示

配置“补丁服务器地址”和“补丁检查不合格提示”信息，该补丁服务器地址只用于告知终端用户补丁服务器的地址，便于手工下载补丁，“补丁检查不合格提示”信息，在补丁检查不合格的时候会下发给 iNode 客户端提醒用户。

(b) 手工检查不支持对 Windows 应用软件，如 Windows Media Player，Microsoft Office 等和其他软件(如奇虎、360 等)的补丁检查。

说明 2：当前补丁管理只支持自动联动 WSUS 补丁服务器对 Windows 终端 PC 做补丁检查。

补丁检查具体步骤：第一，用户上网前，由接入设备控制将该用户的访问权限限制到隔离区内。EAD 客户端首先向 EAD 策略中心发起安全认证请求。第二，EAD 策略中心根据用户角色下发要求进行补丁检查指令。第三，AD 客户端收到补丁检查指令，首先判断是否定制了简易补丁功能，如果定制了，就开始使用内置的补丁检查接口检查补丁是否及时更新，并将检查结果发送给 EAD 策略中心，如果合格，EAD 策略中心通知接入设备，将该用户的访问权限从隔离区放开，用户可以正常访问其他授权的网络资源。第四，如果不合格，用户依然被限制在隔离区内，只能访问补丁服务器等安全资源，因此不会受到外部病毒和攻击的威胁。同时客户端自动过渡到补丁自动升级阶段。第五，由用户根据补丁更新过程中出现的情况按提示进行相关的操作(如：重启机器等)，确认完成补丁升级后，由用户干预通过 EAD 客户端界面再次发起安全认证，重新检测补丁安装情况，如果合格，则放开用户访问权限。

测试 WSUS 补丁服务器是否可用的最简单方法是用一台没有更新补丁的 PC 接入能访问 WSUS 的网络，观察能否正常更新补丁。

② 授权配置检查。当终端不满足安全策略时，会将该用户下线或者放到隔离区，而隔离区的构造通常通过下发 ACL 或 VLAN 实现，在使用 ACL 或 VLAN 进行授权场景，需要确保下发后终端 PC 和策略服务器能正常通信。

例如：终端 PC：192.168.100.1，策略服务器：172.16.100.200，补丁服务器：172.16.100.210 如果使用 ACL 进行授权，则设备侧的 ACL 配置中必须有放通源 IP：192.168.100.1，目的 IP：172.16.100.200 和 172.16.100.210 的 rule，如图 8-363 所示。

```
acl number 3000
rule 0 permit ip source 192.168.100.1 0 destination 172.16.100.200 0
rule 1 permit ip source 192.168.100.1 0 destination 172.16.100.210 0
rule 2 deny ip
```

图 8-363　终端 PC

如果 ACL 是下发给 iNode 客户端，服务器侧的客户端 ACL 配置中也必须有放通目的 IP 为策略服务器和补丁服务器的规则，如图 8-364 所示。

EAD 构造隔离区有下发 ACL 和 VLAN 两种，而 ACL 可以下发给设备，也可以下发给 iNode 客户端。VLAN 只能下发给设备，向接入设备下发接入用户所使用的 VLAN，可以下



图 8-364　策略服务器和补丁服务器

发 VLAN ID，也可以下发 VLAN NAME，如果下发 VLAN ID，则 VLAN ID 必须在 1～4094 之间，如果接入设备上不存在此 VLAN ID，则会自动创建，如果下发 VLAN NAME，接入设备上必须预先创建此 VLAN NAME，否则下发的 VLAN 无效。如果 ACL 下发给设备，则必须预先在设备侧配置好 ACL，如果 ACL 下发给 iNode 客户端，则 ACL 规则需要在 iMC 服务器侧配置，并且 iNode 需要定制客户端 ACL 功能，如图 8-365 所示。

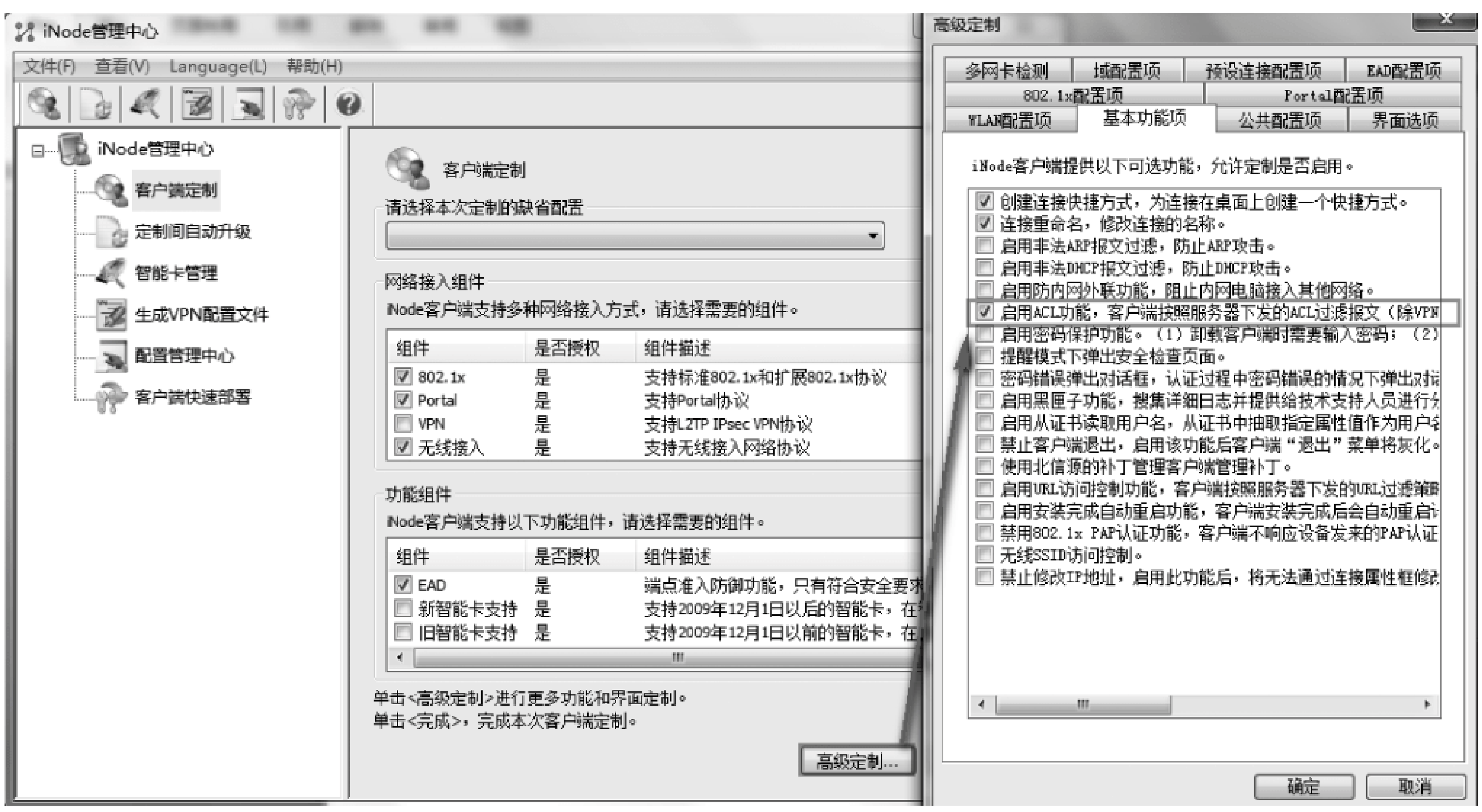


图 8-365　高级定制

(4) 终端 PC 补丁安装情况检查

在实施 EAD 补丁检查策略之前，为了不影响正常业务，请确保各终端满足补丁检查策略要求，更新要求的补丁版本，可以通过单击“控制面板”→“程序”→“查看已安装的更新”命令来查看已经下载更新的补丁，如图 8-366 所示。

本例使用 Windows 7 进行举例，不同操作系统查看补丁方式可能不同。

(5) 终端 PC 补丁自动更新开关检查

在结合 WSUS 补丁服务器检查补丁场景，需要手工开启终端 PC 的补丁自动更新服务，否则无法自动更新补丁，补丁检查时会提示补丁更新失败，启动补丁自动更新服务的方法：单击“控制面板”→“管理工具”→“服务”命令，启动名称为“Windows Update”的服务，如图 8-367 所示。

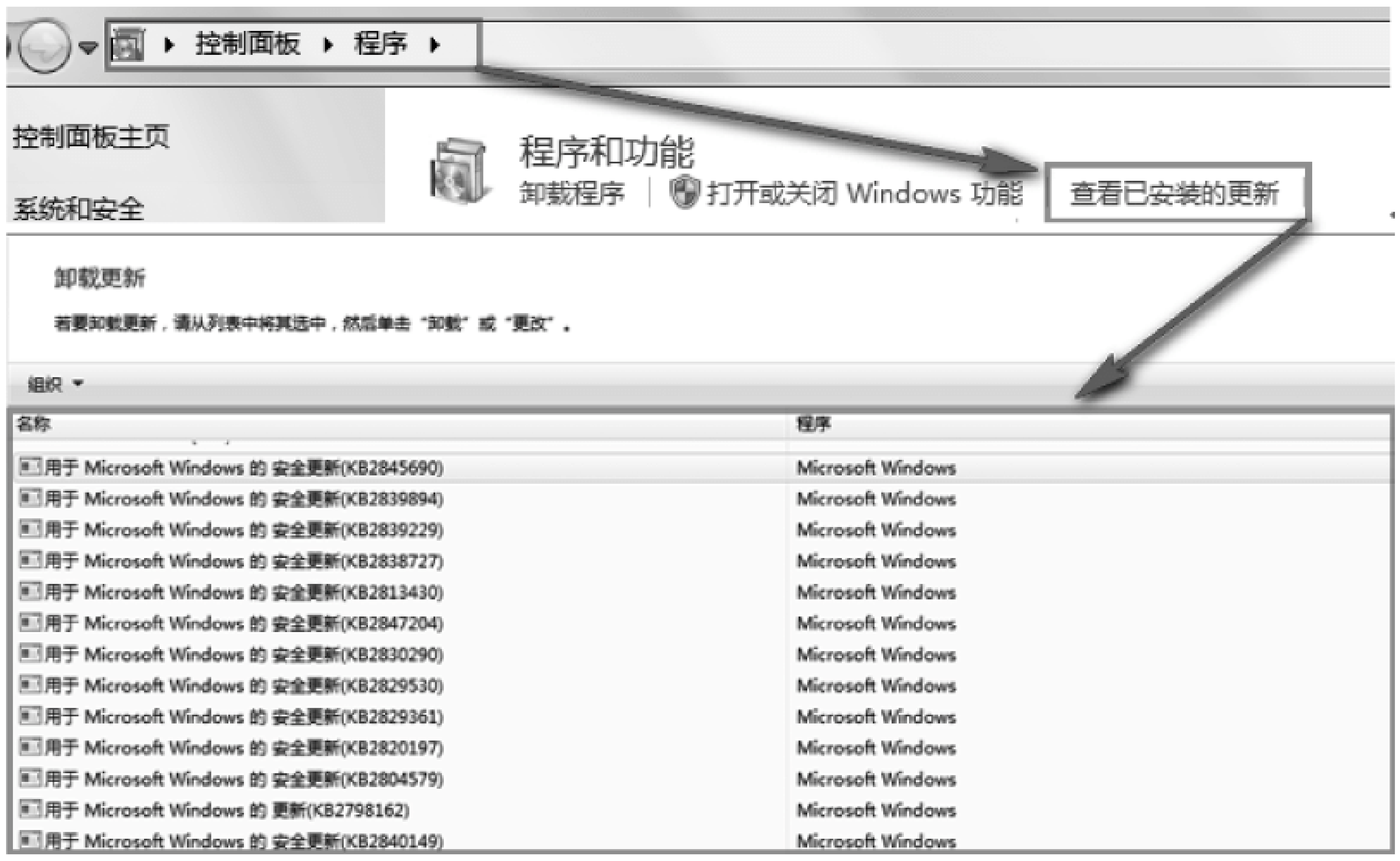


图 8-366 PC 补丁安装情况

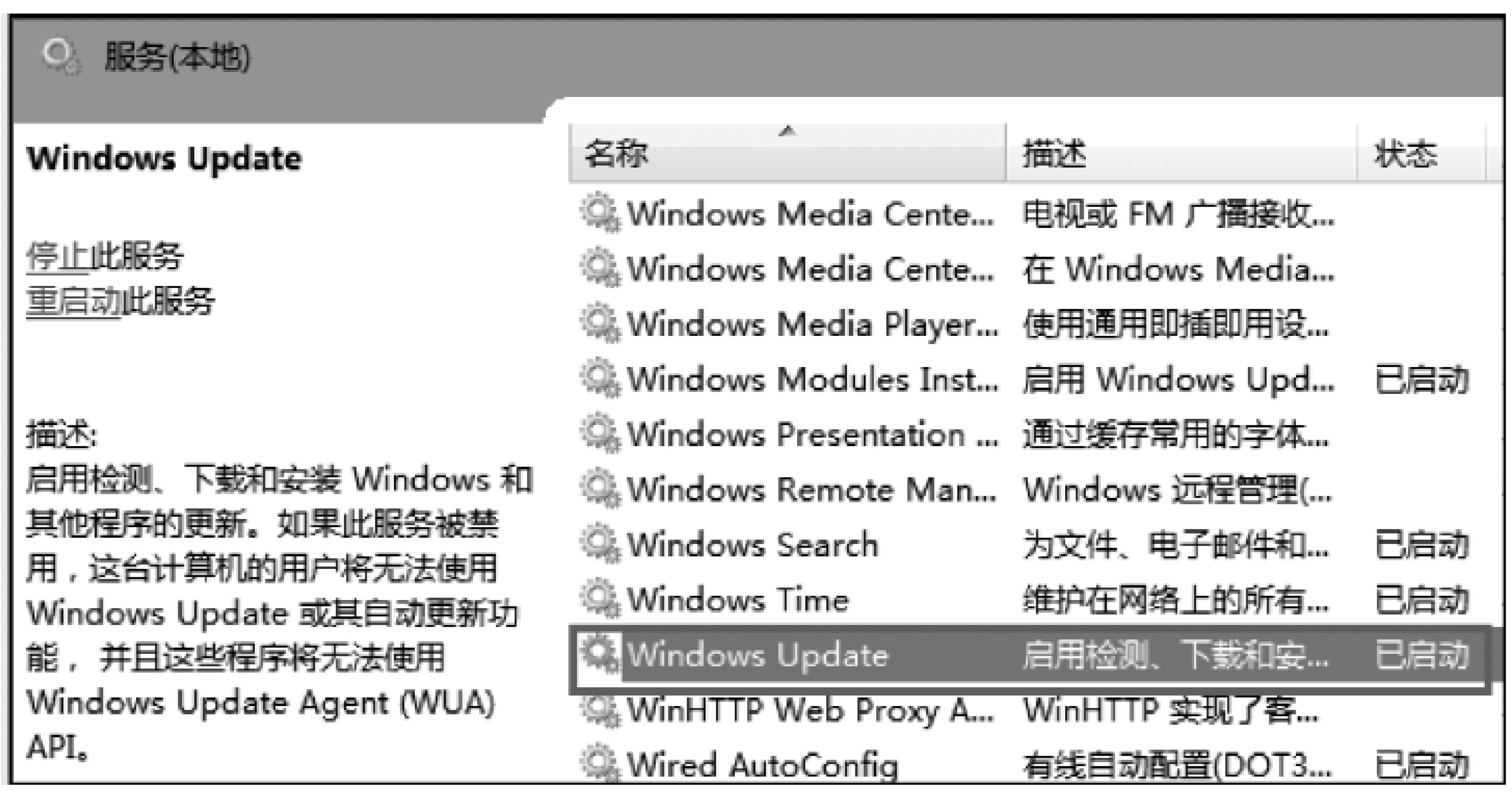


图 8-367 PC 补丁自动更新

(6) iNode 定制功能和支持列表检查

如果需要做 EAD，终端 PC 必须要安装 H3C iNode 客户端，首先检查 iNode 是否定制了 EAD 功能，然后检查当前的 iNode 客户端是否支持补丁检查相关功能。

具体排查方法如下。

H3C iNode 包含 iNode PC 和 iNode DC 两种。

① 查看 iNode PC 是否定制了 EAD 功能：单击 iNode 菜单“信息”→“主机和网络相关信息”命令，打开如图 8-368 所示对话框，查看“客户端信息”标签，是否支持 EAD。

② iNode DC 即可溶解客户端，是 iNode PC 的一个子集，在 Portal 认证场景，如果未安装 iNode PC，但是要实施 EAD，则需要安装部署可溶解客户端，iNode DC 必须先在 iMC 服务器侧安装部署成功后才能使用，如图 8-369 所示。

另外，查看 iNode 的版本说明书，仔细阅读关于补丁检查的限制和注意事项。

(7) PC 和策略服务器连通性检查

在开启策略服务器场景，即使没有做安全检查，也需要确保终端 PC 和策略服务器能正常双向通信，否则，身份认证成功后会下线，其采用 UDP 协议进行通讯，策略服务器使用固定

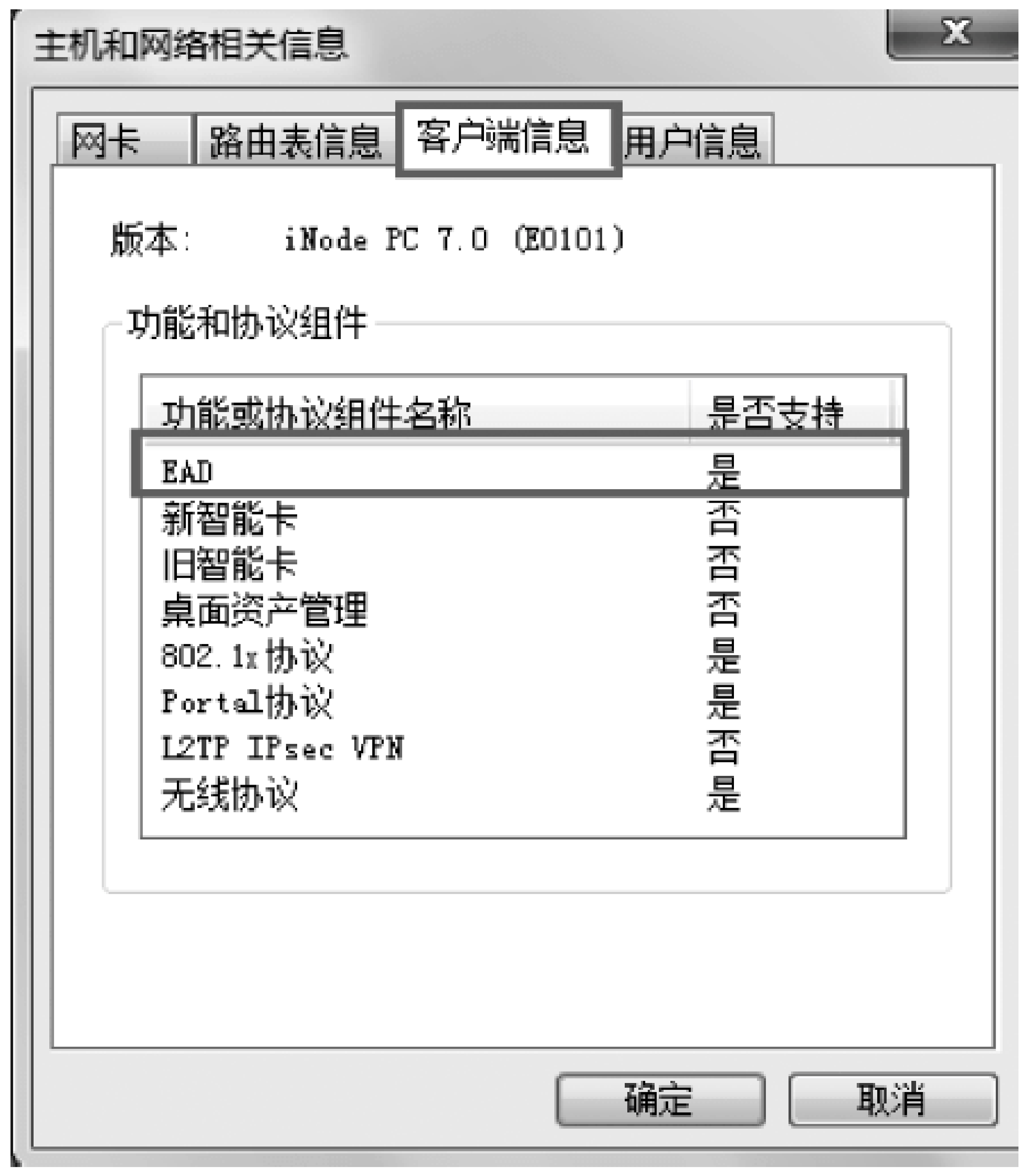


图 8-368 “客户端信息”标签

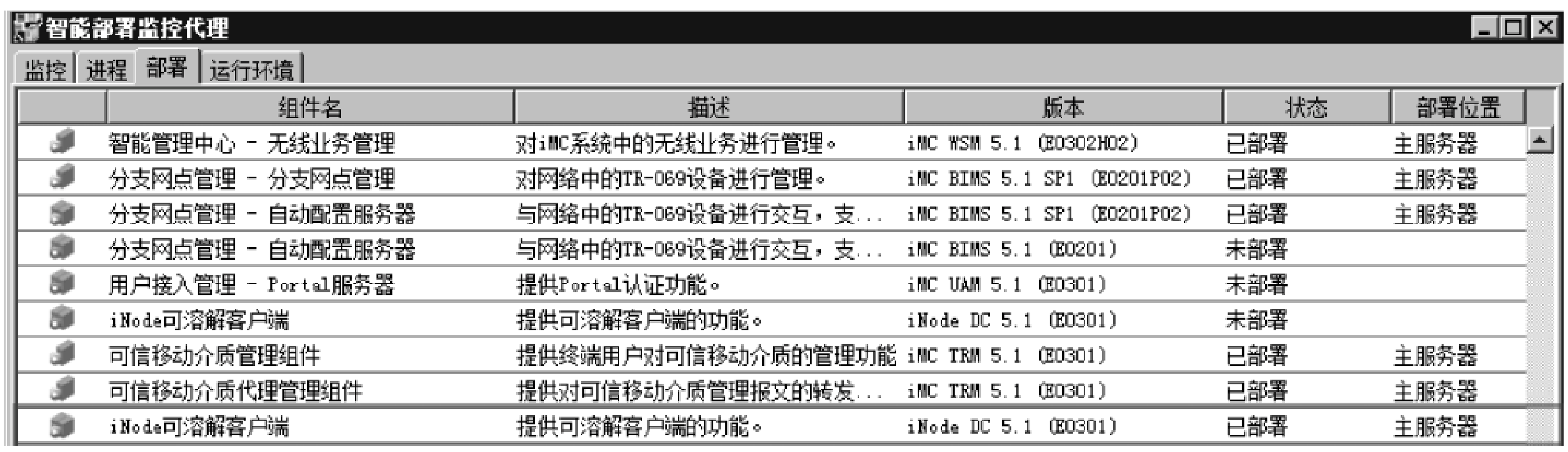


图 8-369 iNode DC 在 iMC 服务器侧安装部署成功

(默认为 9019)端口监听客户端消息,iNode 客户端也从固定监听端口(从 10102 开始递增的第一个空闲端口)发送和接受报文。如果中间有防火墙,需要放通 UDP 协议报文。对于没有禁 ping 的环境,从 iMC 服务器上 ping 终端 PC 的 IP。

对于禁 ping 的环境,有两种方法确定 PC 和策略服务器的连通性。

① 可以在策略服务器和终端 PC 侧同时抓包确定是否能正常通信,如图 8-370 所示。

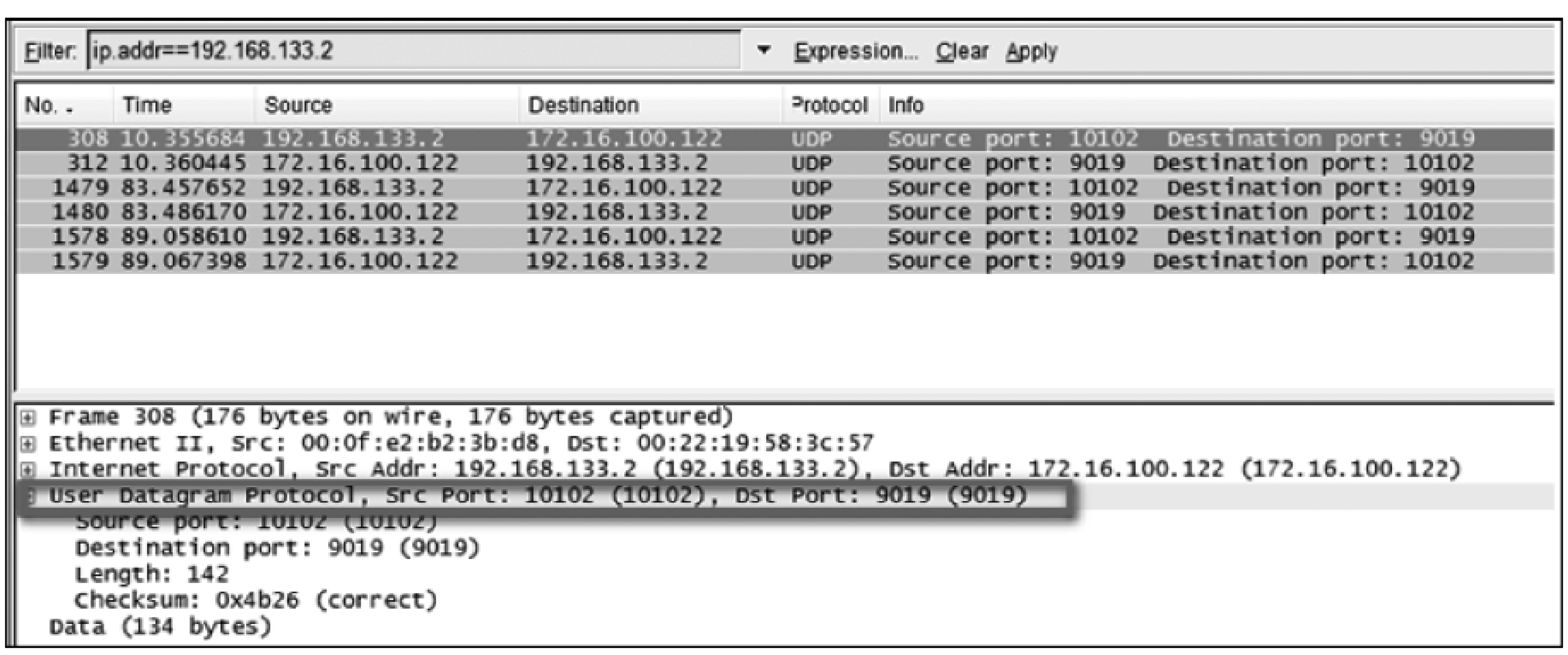


图 8-370 确定是否正常通信

说明：如图 8-370 所示，192.168.133.2 为终端 PC 的 IP，172.16.100.122 为策略服务器的 IP，在服务器和 PC 侧同时抓包可以看到其 UDP 报文的详细交互过程。

② 通过 iNode 和策略服务器的日志确定。

iNode 的 Detail 日志文件 secpkt.txt 如下。

```
[2012-02-10 10:42:26] [DtlCmn] [674] secPushInner: out-pkt [1]          //安全认证请求报文
<i n="userName">szh1@iMC</i>
<in="hwAddr">18:A9:05:DF:D4:0E</i>
<i n="eventSeqID">JOvPBgcC</i>
[2012-02-10 10:42:27] [DtlCmn] [1ba0] sndSecMsg: transfer [2] [11260] //安全认证回应报文
<i n="heartBeatInterval">720</i>
<i n="heartBeatOutTimes">3</i>
```

策略服务器调试日志如下。

```
2012-02-10 08:57:38 [策略服务器] [信息(0)] [24] [ProxyRequestHandler::run] szh1@iMC ; EAD
认证上线请求报文(1) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2;...文解析成功
                                                                        //认证上线请求报文
2012-02-10 08:57:38 [策略服务器] [信息(0)] [15] [RequestProcessor::processRequest] szh1@iMC
; EAD 认证上线回应报文(2) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ;   192.168.133.2 ;   ...
                                                                        //认证上线回应报文
```

说明：如上的 iNode 日志级别需要设置为 Detail 才能看到具体的交互报文（日志存放路径：C:\Program Files\H3C\iNode Client\CollectInfo\ *），同理，策略服务器日志级别也需要设置调试才能看到和 iNode 的详细报文交互（日志存放路径：iMC 安装目录\ead\logs\policyserver_ **** - ** - **）；关于日志级别的设置方法请参考其他文档。

(8) PC 和 WSUS 补丁服务器的连通性排查

对于没有禁 ping 的环境，从终端 PC 直接 ping 补丁服务器，对于禁 ping 的环境，如果 iNode 客户端 EAD 认证时提示"补丁检查失败"，可查看终端 PC 的 C:\Windows 目录下的 Windows Update 日志文件，根据日志文件提示信息的错误码，然后再上微软的网站 http://support.microsoft.com 或其他网址查找"0x80072EFD"这个错误码的含义以及解决方法。

日志提示信息：2013-05-2908:53:28:143 908e48Agent ************* 2013-05-2908:53:28:143 908e48AgentWARNING：WU client failed Searching for update with error 0x80072efd 微软官网问题原因："如果在检查更新时收到 Windows Update 错误 80072efd，可能是因为计算机与 Windows Update 服务器之间的连接中断引起的。"

解决方法：关闭 Windows Update，等待 10～15 分钟，然后再次运行 Windows Update。你也可以等待 Windows Update 在其下次计划时间运行。具体操作步骤：①单击此按钮：。②在"文件下载"对话框中，单击"运行"按钮，然后执行向导中的步骤。③打开 Windows Update，尝试再次安装更新。如果仍然收到此错误，这可能意味着你的计算机中所运行的某个程序阻止了 Windows Update 服务（SVCHOST）访问 Internet。这样的程序包括防火墙、反间谍软件、Web 加速器、Internet 安全或防病毒程序以及代理服务器。若要解决该问题，可能需要将 Windows Update 网站地址添加到阻止程序的例外列表或允许列表，或者允许 Windows Update 服务通过端口 80 和端口 443 连接到 Internet。将 Windows Update 网站添加到防火墙例外列表 Windows 防火墙是该版本 Windows 附带的防火墙，其例外列表中应当已包括这些站点。如果使用其他防火墙，请参阅软件发布者的文档，查看如何将这些网站添加

到防火墙例外列表中。

(9) 身份认证测试

身份认证成功后才会发起安全认证,在 EAD 安全认证前,必须确保能身份认证成功,如图 8-371 所示。

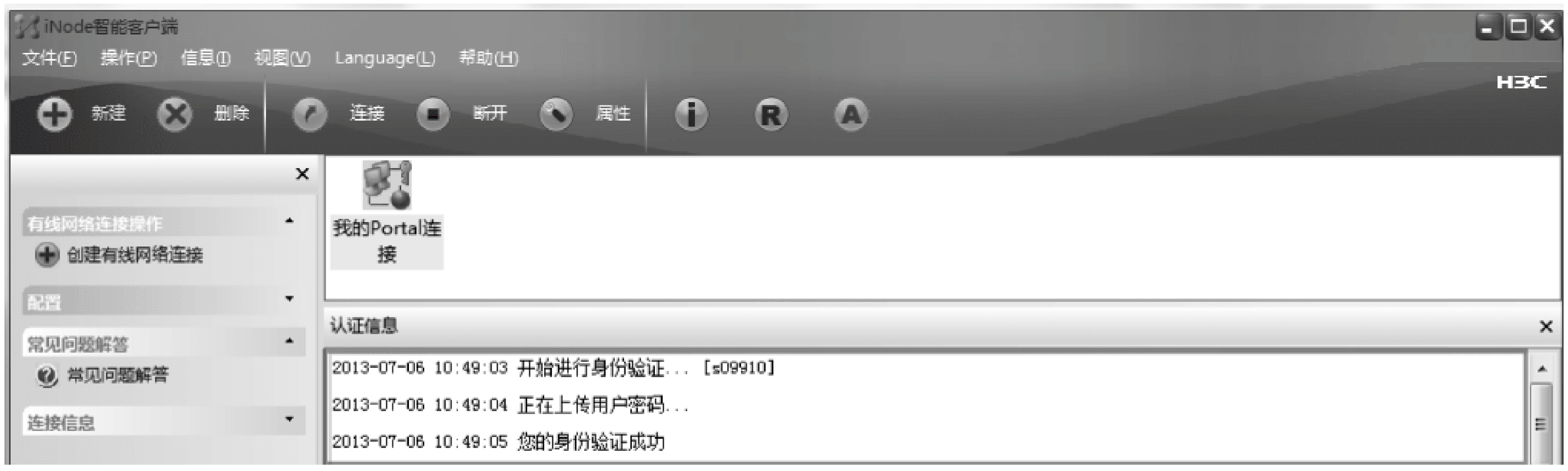


图 8-371　身份认证测试

如果身份认证失败,请参考身份认证相关云图。

(10) 接入设备配置排查

如果身份认证成功后,却一直未触发安全认证,这里就需分两种情况讨论。

① 如果接入设备是 H3C 类型,在 Portal+EAD 场景,则设备侧的 Radius Scheme 方案里的 Server-type 配置 Extended|Standard 都可以。在 Dot1x+EAD 场景,则 Radius Scheme 方案里的 Server-type 可以配置 Standard,但是 Dot1x Authencation-method 必须配置为 EAP 才能触发 EAD 认证,但是无法给设备下发 ACL 和 VLAN 进行授权,如果 ACL 下发给 iNode 不受影响,故接入设备是 H3C 类型,在 EAD 开局中,建议将 Radius Scheme 的 Server-type 配置为 Extended。

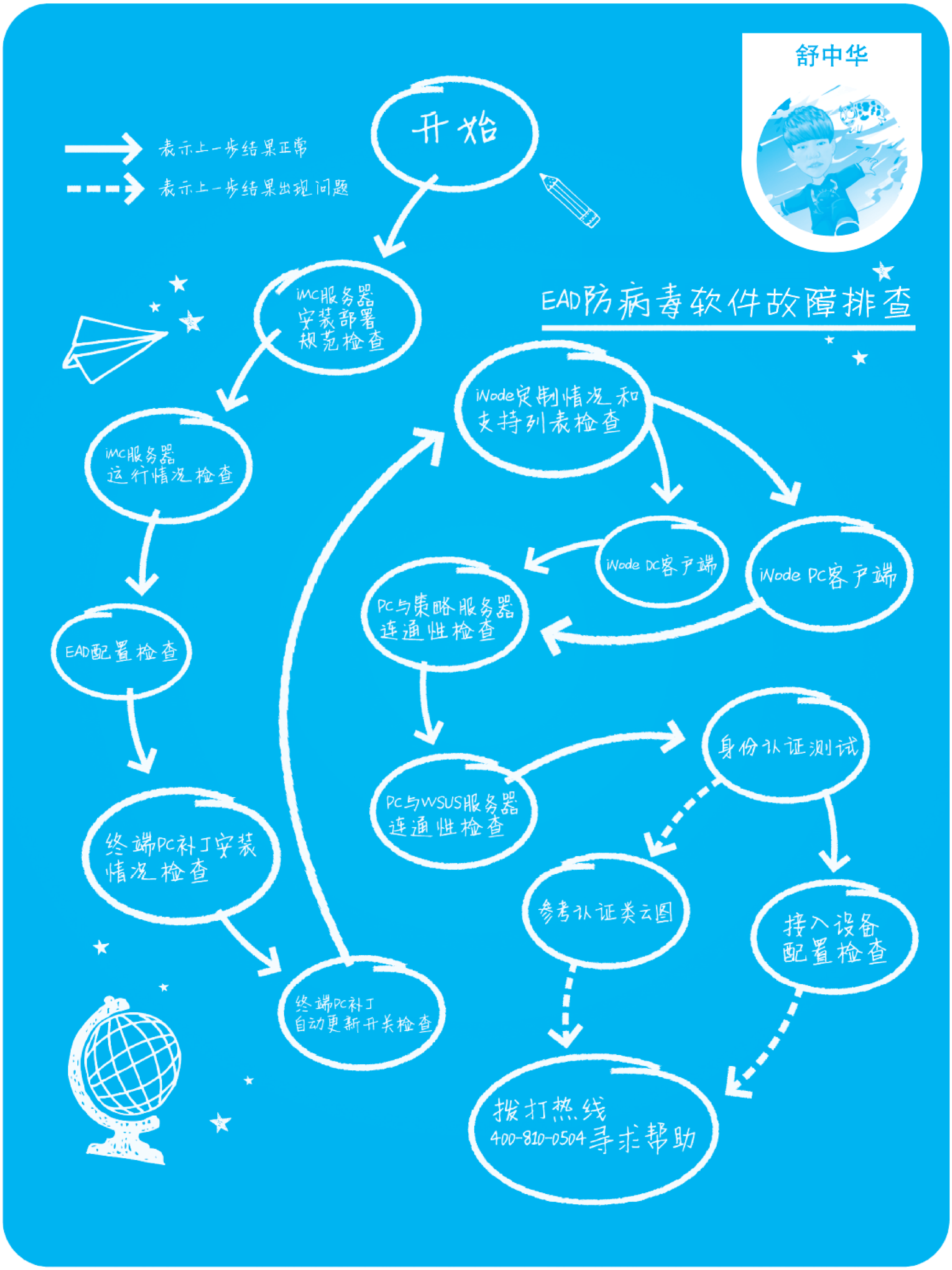
② 如果接入设备是第三方厂商,由于不支持 Portal 认证,在 802.1x 认证场景 Authentication-method 必须配置为 EAP 方式,否则不会触发安全认证。H3C 设备配置方法如图 8-372 所示。

```
radius scheme test
 server-type extended
```

```
[ywrj-121-C0re]dot1x authentication-method eap
 EAP authentication is enabled
```

图 8-372　H3C 设备配置方法

说明:结合第三方设备实施 EAD 解决方案,Dot1x+EAD 场景,Dot1x authentication-method 必须配置为 EAP,如果是 L2TP VPN+EAD,则接入设备必须为 H3C 设备,因为第三方设备的 Radius Scheme 不支持 Extended,且 VPN 认证方式不支持 EAP,故不支持 EAD。


舒中华
表示上一步结果正常
表示上一步结果出现问题
开始
EAD防病毒软件故障排查
iMC服务器安装部署规范检查
iMC服务器运行情况检查
EAD配置检查
终端PC补丁安装情况检查
终端PC补丁自动更新开关检查
iNode定制情况和支持列表检查
iNode DC客户端
iNode PC客户端
PC与策略服务器连通性检查
PC与WSUS服务器连通性检查
身份认证测试
参考认证类云图
接入设备配置检查
拨打热线
400-810-0504寻求帮助

1. 开始

EAD 防病毒软件管理可以将不符合安全要求的终端踢下线或限制在“隔离区”内，防止“危险”终端对网络安全的损害，避免“易感”终端受病毒、蠕虫的攻击。

EAD 防病毒软件管理排错思路：身份认证之后才会触发安全认证，关于身份认证失败的排查思路可以参考具体的认证类云图，在此不再叙述。

首先检查服务器软硬件及性能是否满足当前认证需要，然后从 iNode PC 和 iNode DC 两种客户端认证场景进行分析，相应做 iMC 服务器运行状态的检查，安全策略配置检查，终端防病毒软件安装情况检查，最后对 iNode 支持的防病毒软件版本进行确认。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“EAD 安全策略管理”各组件是否已部署的状态，具体如图 8-373 所示，关于“用户接入管理”组件的检查方式，请参考认证类云图。



组件名	描述	版本	状态
网络流量分析服务	对网络流量信息提供多角度的统计...	iMC NTA 5.2 (E0401)	未部署
用户行为审计服务	提供对多种用户行为日志的管理功能。	iMC UBA 5.2 (E0401)	未部署
服务健康管理 - NQA采集器管理	采集并分析设备上网络性能相关的...	iMC SHM 5.2 (E0401)	未部署
用户接入管理 - 用户接入管理	提供对接入用户、接入业务的配置...	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - Portal服务器	提供Portal认证功能。	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - BYOD服务器	提供BYOD的功能。	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - 策略服务器	提供安全认证的功能。	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - 策略代理服务器	提供对安全认证报文的转发功能。	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - 用户自助服务	提供用户资料的自助查询和维护的...	iMC UAM 5.2 (E0402P05)	已部署
用户接入管理 - 用户接入管理从服务器	部署在用户接入管理服务器之外的...	iMC UAM 5.2 (E0402)	未部署
EAD安全策略管理 - 安全策略管理前台	提供对EAD业务的配置功能。	iMC EAD 5.2 (E0402P05)	已部署
EAD安全策略管理 - 桌面资产管理	提供对桌面资产业务的配置和用户...	iMC EAD 5.2 (E0402P05)	已部署
EAD安全策略管理 - 桌面资产管理代...	提供对桌面资产管理报文的转发功能。	iMC EAD 5.2 (E0402P05)	已部署

图 8-373 组件部署状态

说明：EAD 安全策略管理—桌面资产管理和 EAD 安全策略管理—桌面资产管理代理服务器是桌面资产(DAM)管理的功能组件，在 EAD 解决方案中可以不部署。

(2) iMC 服务器运行情况检查

要顺利实施 EAD 解决方案，除了确保 UAM 相关进程运行正常外，还要检查策略服务器对应的进程是否运行正常，及进程绑定的端口是否正常，具体可从如下两方面检查。

① 单击“开始”→“智能部署监控代理”命令，选择“进程”标签，查看 EAD 的核心进程 policyserver 是否正常启动，具体如图 8-374 所示。



图 8-374 进程启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

② 检查策略服务器对应的监听端口 UDP 9019，UDP 9017 是否正常绑定，如图 8-375 所示。

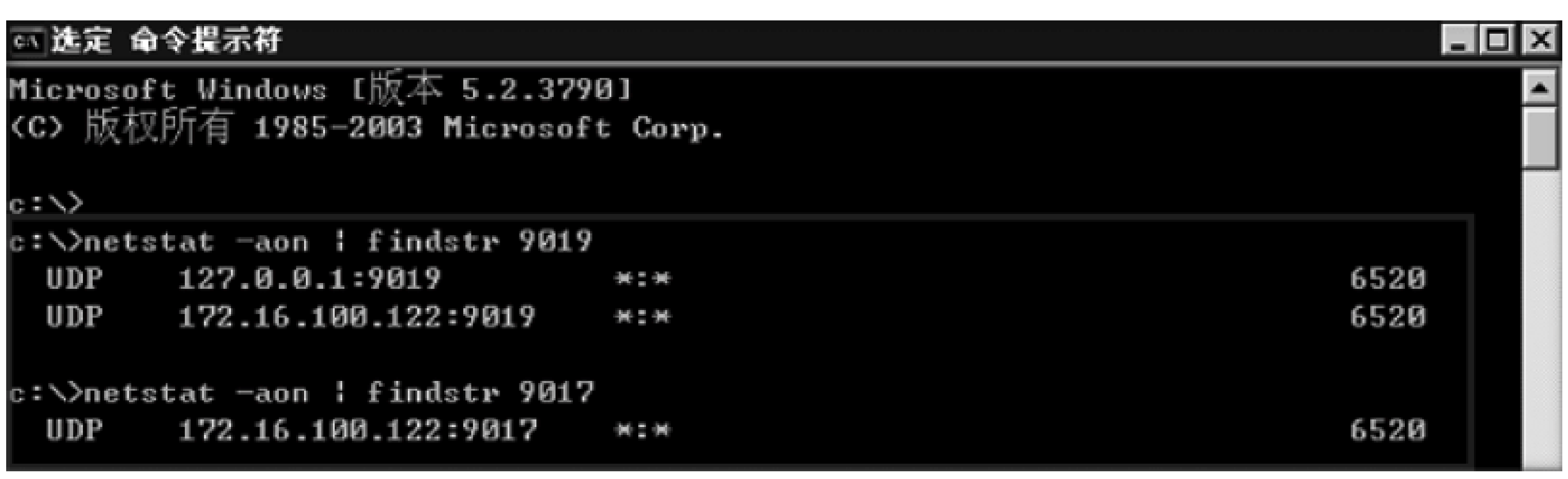


图 8-375 各端口正常绑定情况

说明 1：如图 8-375 所示，9019 端口号必须同时绑定两个 IP，分别是 127.0.0.1 和实际网卡 IP:172.16.100.122，而 9017 端口只需绑定实际网卡 IP 即可，如图 8-376 所示。

说明 2：Windows 操作系统中，通过命令 netstat -aon |findstr 端口号来显示某端口的监听状态以及对应的进程 PID，举例，对应提示符回显如图 8-377 所示。

其中第一列 UDP 监听的协议；第二列 172.16.100.122：9017 所指监听的服务器的 IP 和端口号；第三列 *.* 代表监听状态；最后一列 6520 代表此协议监听的进程 PID，根据此 PID，对照 Windows 任务管理器，即可确定该端口绑定的具体服务。



图 8-376　绑定两个 IP



图 8-377　提示符回显

(3) EAD 配置检查

① 安全策略配置检查。

要实施防病毒软件管理，首先必须配置防病毒软件策略，比如，要检查“金山毒霸网络版”，则必须创建一个策略，并在策略中勾选检查项的复选框，如图 8-378 所示。



图 8-378　配置防病毒软件策略

然后创建安全策略，并在安全策略中将创建的防病毒软件策略和安全级别绑定，然后在“服务”里绑定“安全策略”，最终，接入账号和服务进行绑定，总之，只有账号绑定了正确的“服务”，“服务”绑定了正确的“安全策略”，“安全策略”绑定了正确的“安全级别”和“防病毒软件策略”，才会进行防病毒软件的检查。

检查账号是否配置了正确的安全策略最直观的方法。

通过接入账号确定其绑定的服务，然后通过服务确定其绑定的安全策略，通过安全策略确定具体的防病毒策略和安全级别，安全级别是下线、隔离、提醒，还是监控，下发的 ACL，VLAN 配置是否正确等，如图 8-379、图 8-380 所示。

一个防病毒软件策略，同时勾选了多个防病毒软件，如图 8-381 所示，同时勾选了“360 卫

士”和“360MobileSafe”，则会按照优先级由高往低顺序进行检查，在检查过程中，只要检测到不满足的防病毒软件，会立即终止检查，即安全检查不通过，也就是说，安全认证失败场景，iNode 侧的认证信息可能不会回显所有已装的安全软件，故在配置防病毒软件策略时，必须按实际要求勾选对应的防病毒软件检查项。



图 8-379　直观方法

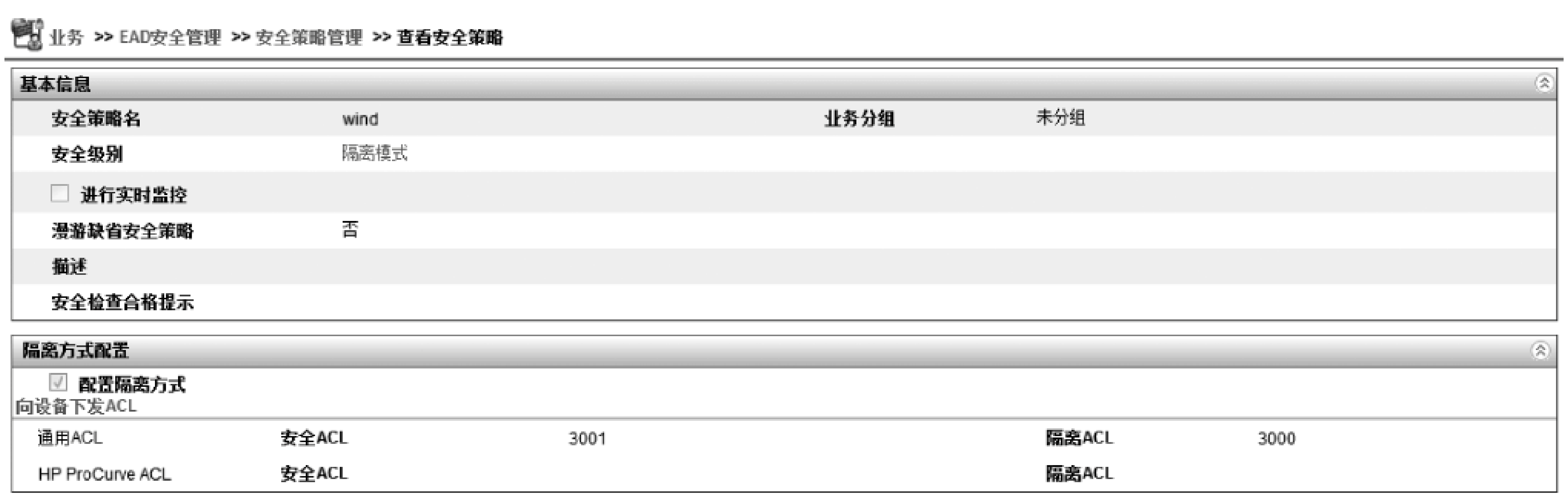


图 8-380　ACL 配置正确情况



图 8-381　防病毒软件设置窗口

说明：iNode 检查终端 PC 有没有安装某安全软件，只查看 PC 侧“卸载或更改程序”已安装软件的名称和 EAD 服务器侧“防病毒软件”的名称是否一致，如果不一致，即使终端 PC 安装了安全软件，EAD 服务器也会提示没有安装所要求的防病毒软件。

② 防病毒软件名称一致性检查。

EAD 可以检查终端 PC 是否安装所要求的安全软件，以及具体的程序版本号，病毒库版本号以及引擎版本，在身份认证成功后，如果提示未安装要求的安全软件，请检查终端 PC 是否有正常安装好相关安全软件，如果安装成功，则检查终端 PC 侧“控制面板”→“卸载或更改程序”中已安装软件的名称和 iMC 服务器侧配置项：单击“业务”→“EAD 安全软件”→“终端安全软件策略管理”→“防病毒软件策略管理”→“修改防病毒软件策略”→“防病毒软件设置”命令后的名称是否一致，如果不一致，请修改和终端 PC 一致即可，如图 8-382、图 8-383 所示。



图 8-382　终端 PC“卸载或更改程序”窗口查看防病毒软件名称

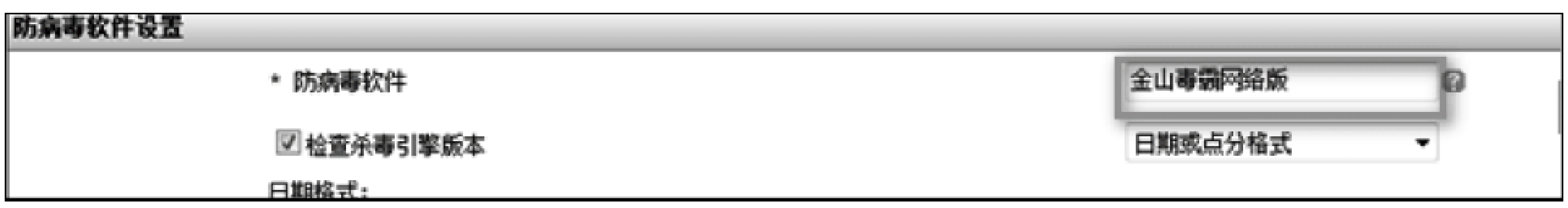


图 8-383　防病毒软件设置窗口

③ 授权配置检查。

当终端不满足安全策略时，会将该用户下线或放到隔离区，而隔离区的构造通常通过下发 ACL 或 VLAN 实现，在使用 ACL 或 VLAN 进行授权场景，需要确保下发后终端 PC 和策略服务器能正常通信。

例如：终端 PC：192.168.100.1，策略服务器：172.16.100.200，如果使用 ACL 进行授权，则设备侧的 ACL 配置中必须有放通源 IP：192.168.100.1，目的 IP：172.16.100.200 的 rule，如图 8-384 所示。

```
acl number 3000
 rule 0 permit ip source 192.168.100.1 0 destination 172.16.100.200 0
 rule 1 deny ip
```

图 8-384　终端 PC

如果 ACL 是下发给 iNode 客户端，服务器侧的客户端 ACL 配置中也必须有放通目 IP 为策略服务器 172.16.100.200 的规则，如图 8-385 所示。

说明：EAD 构造隔离区有下发 ACL 和 VLAN 两种，而 ACL 可以下发给设备，也可以下发给 iNode 客户端，VLAN 只能下发给设备，向接入设备下发接入用户所使用的 VLAN，可以下发 VLAN ID，也可以下发 VLAN NAME，如果下发 VLAN ID，则 VLAN ID 必须在 1～4094 之间，如果接入设备上不存在此 VLAN ID，则会自动创建，如果下发 VLAN NAME，接入设备

上必须预先创建此 VLAN NAME，否则下发的 VLAN 无效。如果 ACL 下发给设备，则必须预先在设备侧配置好 ACL，如果 ACL 下发给 iNode 客户端，则 ACL 规则需要在 iMC 服务器侧配置，并且 iNode 需要定制客户端 ACL 功能，如图 8-386 所示。



图 8-385　策略服务器规则

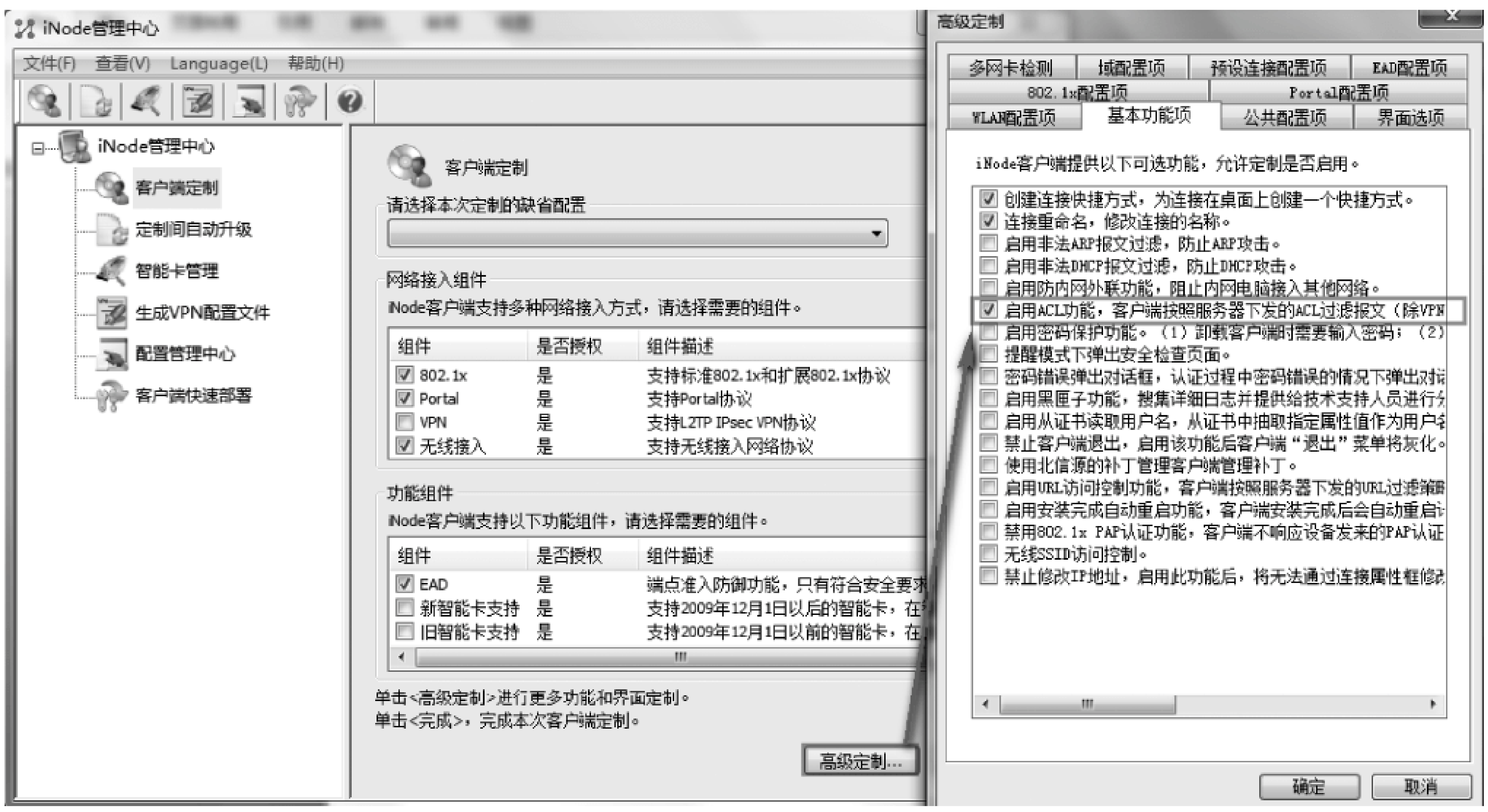


图 8-386　高级定制

(4) 终端 PC 防病毒软件安装情况检查

EAD 防病毒管理可以检测终端 PC，包括 Windows、Linux、Mac OS，以及智能终端 Android 是否安装满足的安全软件，包括软件版本，引擎版本，故终端 PC 必须安装满足安全策略要求的防病毒软件及其版本。查看终端防病毒软件的安装情况以及版本方法：单击"控制面板"→"程序"→"程序和功能"命令查看已安装的防病毒软件版本，也可直接打开终端 PC 安装的防病毒软件查看程序版本和病毒库版本，如图 8-387 所示。



图 8-387　程序版本及病毒库版本

说明：并不是所有防病毒软件都有引擎版本，比如：360 杀毒软件就没有引擎版本。针对有引擎版本的防病毒软件从程序界面也看不到，需要借助 iNode 客户端获取，iNode 客户端会发起 EAD 请求报文进行安全认证，iNode 客户端的认证信息会显示获取到的防病毒软件的病毒库版本，引擎版本以及程序版本。

(5) iNode 定制功能和支持列表检查

如果需要做 EAD，终端 PC 必须要安装 H3C iNode 客户端，H3C iNode 包含 iNode PC 和 iNode DC 两种。

① 查看 iNode PC 是否定制了 EAD 功能：单击 iNode 菜单"信息"→"主机和网络相关信息"命令后有如图 8-388 所示对话框，查看"客户端信息"标签，是否支持 EAD。

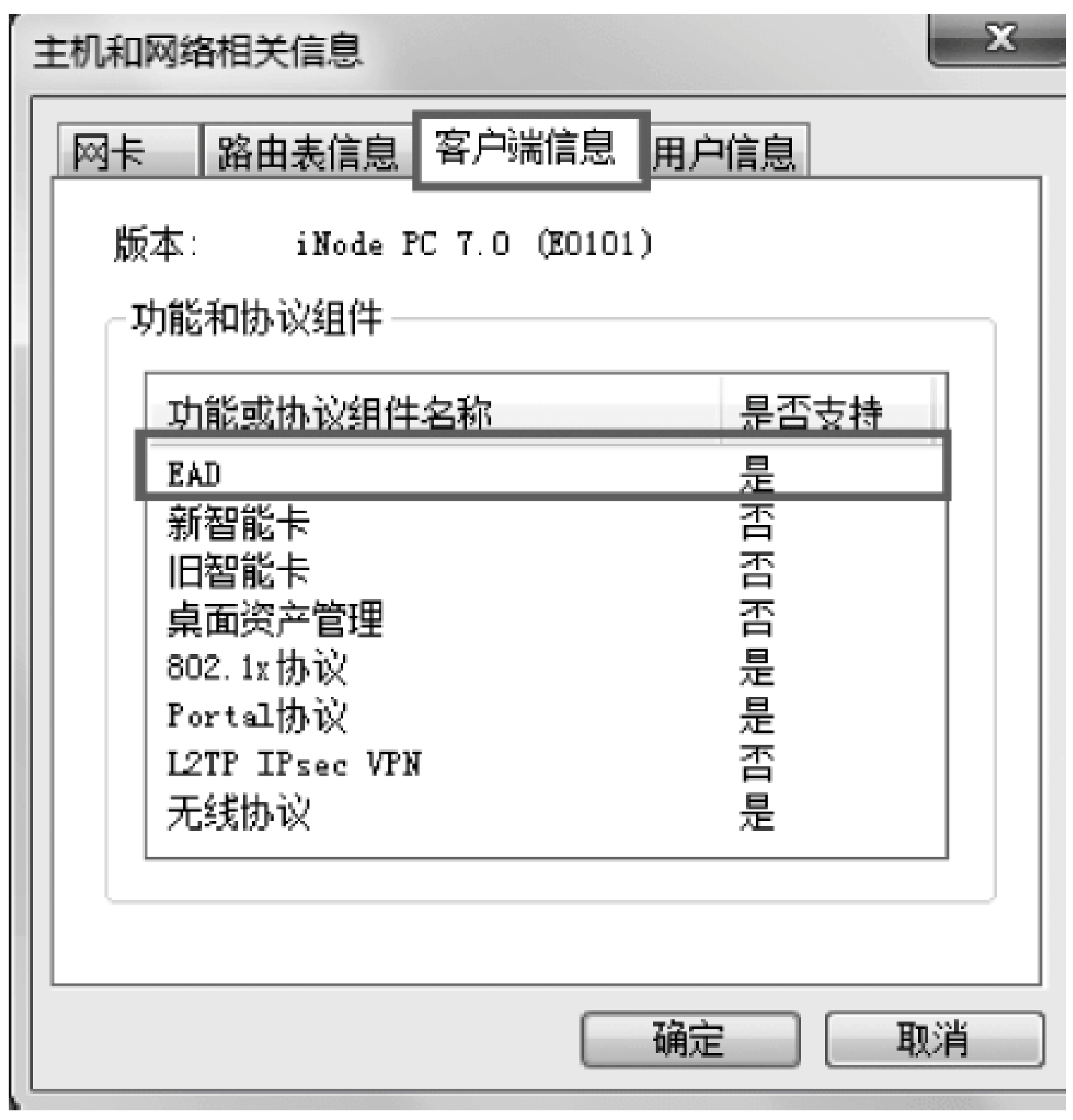


图 8-388 "客户端信息"标签

② iNode DC 即可溶解客户端，是 iNode PC 的一个子集，在 Portal 认证场景，如果未安装 iNode PC，但是要实施 EAD，则需要安装部署可溶解客户端，iNode DC 必须先在 iMC 服务器侧安装部署成功后才能使用，如图 8-389 所示。



图 8-389 iMC 服务器侧安装部署成功

(6) PC 和策略服务器连通性检查

在开启策略服务器场景，即使没有做安全检查，也需要确保终端 PC 和策略服务器能正常双向通信，否则，身份认证成功后会下线，其采用 UDP 协议进行通讯，策略服务器使用固定(默认为 9019)端口监听客户端消息，iNode 客户端也从固定监听端口(从 10102 开始递增的第一个空闲端口)发送和接受报文。如果中间有防火墙，需要放通 UDP 协议报文。对于没有禁

ping 的环境，从 iMC 服务器上 ping 终端 PC 的 IP。

对于禁 ping 的环境，有以下两种方法确定 PC 和策略服务器的连通性。

① 可以在策略服务器和终端 PC 侧同时抓包确定是否能正常通信，如图 8-390 所示。

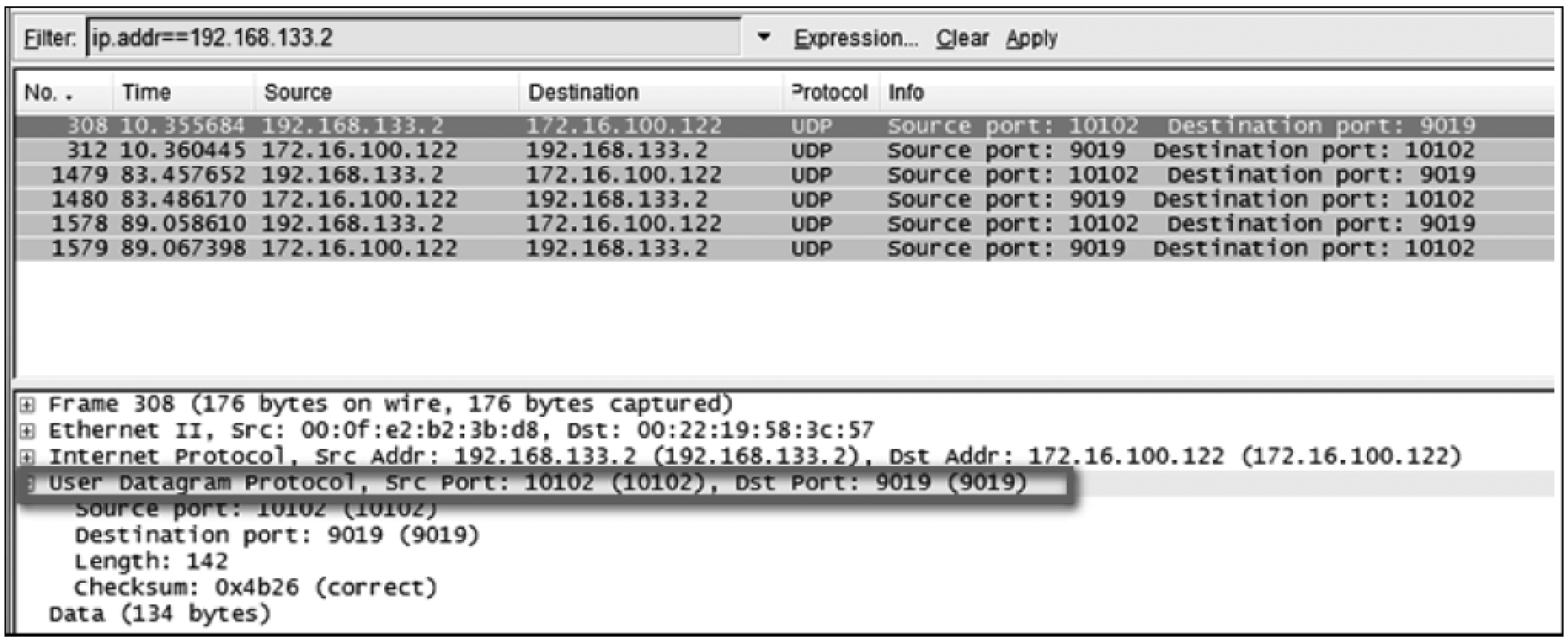


图 8-390 抓包确定正常通信

说明：如图 8-390 所示，192.168.133.2 为终端 PC 的 IP，172.16.100.122 为策略服务器的 IP，在服务器和 PC 侧同时抓包可以看到其 UDP 报文的详细交互过程。

② 通过 iNode 和策略服务器的日志确定，

iNode 的 Detail 日志文件 secpkt.txt 如下。

```
[2012-02-10 10:42:26] [DtlCmn] [674] secPushInner: out-pkt [1]          //安全认证请求报文
<i n="userName">szh1@iMC</i>
<in="hwAddr">18:A9:05:DF:D4:0E</i>
<i n="eventSeqID">JOvPBgcC</i>
[2012-02-10 10:42:27] [DtlCmn] [1ba0] sndSecMsg: transfer [2] [11260]   //安全认证回应报文
<i n="heartBeatInterval">720</i>
<i n="heartBeatOutTimes">3</i>
```

策略服务器调试日志如下。

```
2012-02-10 08:57:38 [策略服务器] [信息(0)] [24] [ProxyRequestHandler::run] szh1@iMC ; EAD
认证上线请求报文(1) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2;...文解析成功
                                                                //认证上线请求报文
2012-02-10 08:57:38 [策略服务器] [信息(0)] [15] [RequestProcessor::processRequest] szh1@iMC
; EAD 认证上线回应报文(2) ; kNIXeLUQ ;18:A9:05:DF:D4:0E;192.168.133.2;...
                                                                //认证上线回应报文
```

说明：如上的 iNode 日志级别需要设置为 Detail 才能看到具体的交互报文(日志存放路径：C\Program Files\H3C\iNode Client\CollectInfo\ *)，同理，策略服务器日志级别也需要设置调试才能看到和 iNode 的详细报文交互(日志存放路径：iMC 安装目录\ead\logs\policyserver_ **** - ** - **)；关于日志级别的设置方法请参考其他文档。

(7) 身份认证测试

身份认证成功后才会发起安全认证，在 EAD 安全认证前，必须确保能身份认证成功，如图 8-391 所示。

如果身份认证失败，请参考身份认证相关云图。



图 8-391　身份认证测试

(8) 接入设备配置排查

如果身份认证成功后，却一直未触发安全认证，这里需分两种情况讨论。

① 如果接入设备是 H3C 类型，在 Portal+EAD 场景，则设备侧的 Radius Scheme 方案里的 Server-type 配置 Extended|Standard 都可以。在 Dot1x+EAD 场景，则 Radius Scheme 方案里的 Server-type 可以配置 Standard，但是 Dot1x Authencation-method 必须配置为 EAP 才能触发 EAD 认证，但是无法给设备下发 ACL 和 VLAN 进行授权，如果 ACL 下发给 iNode 不受影响，故，接入设备是 H3C 类型，在 EAD 开局中，建议将 Radius Scheme 的 Server-type 配置为 Extended。

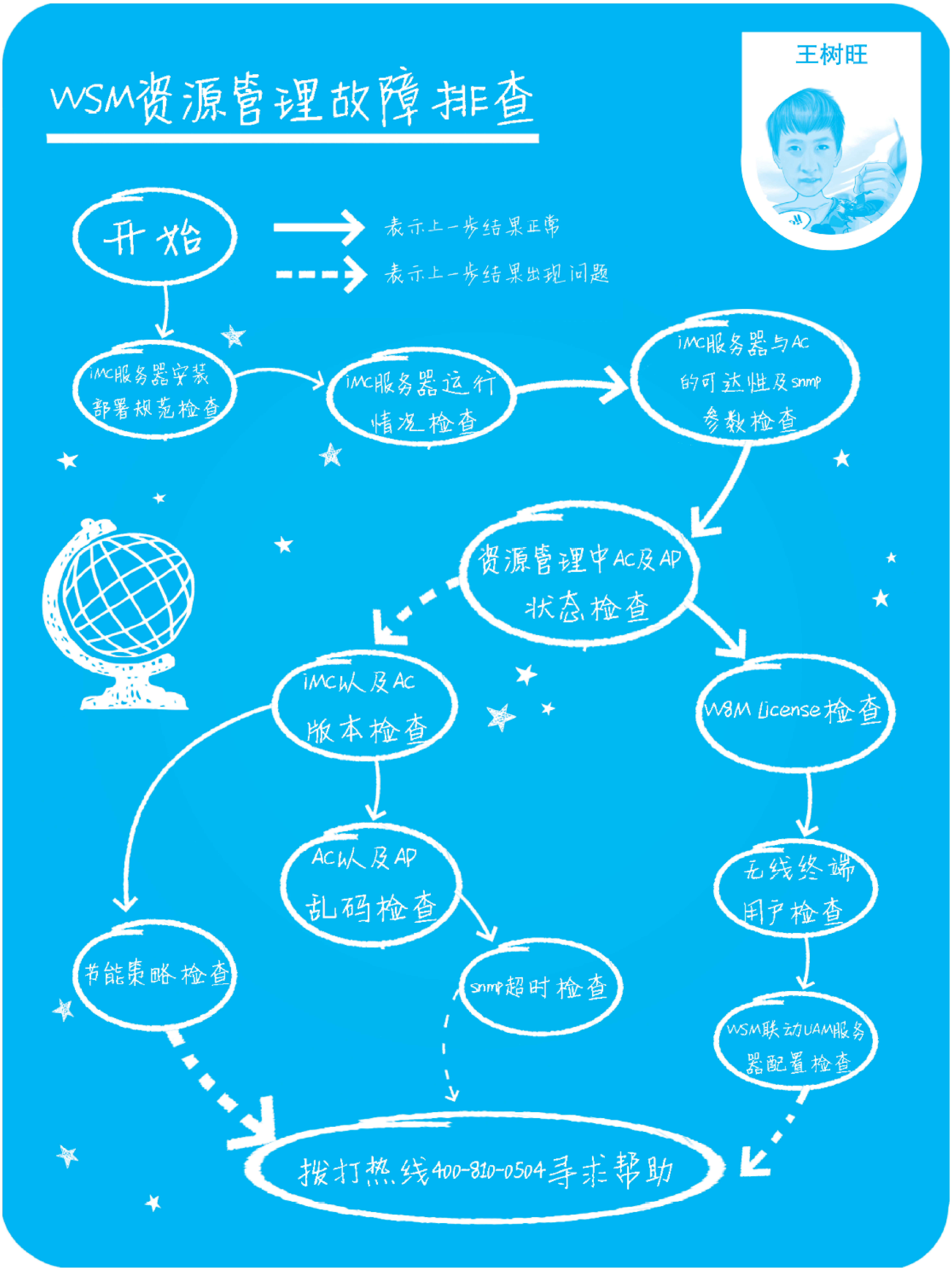
② 如果接入设备是第三方厂商，由于不支持 Portal 认证，在 802.1x 认证场景 Authentication-method 必须配置为 EAP 方式，否则不会触发安全认证。H3C 设备配置方法如图 8-392 所示。

```
radius scheme test
 server-type extended
```

```
[ywrj-121-C0re]dot1x authentication-method eap
 EAP authentication is enabled
```

图 8-392　H3C 设备配置方法

说明：结合第三方设备实施 EAD 解决方案，Dot1x+EAD 场景，Dot1x authentication-method 必须配置为 EAP，如果是 L2TP VPN+EAD，则接入设备必须为 H3C 设备，因为第三方设备的 Radius Scheme 不支持 Extended，且 VPN 认证方式不支持 EAP，故不支持 EAD。


王树旺
WSM资源管理故障排查
开始
表示上一步结果正常
表示上一步结果出现问题
iMC服务器安装部署规范检查
iMC服务器运行情况检查
iMC服务器与AC的可达性及snmp参数检查
资源管理中AC及AP状态检查
iMC以及AC版本检查
WSM License检查
AC以及AP乱码检查
无线终端用户检查
节能策略检查
snmp超时检查
WSM联动UAM服务器配置检查
拨打热线400-810-0504寻求帮助

1. 开始

WSM 资源管理整合了无线设备基础资源管理的各项功能，包括 AC、AP 以及终端用户的状态、资源管理，基于 AP 和客户端的无线定位，无线入侵检测及防护，频谱防护等。WSM 需要与设备侧进行很好的配合，完成上述各业务及功能的管理、检测以及展示。

此流程简洁地描绘了使用 WSM 资源管理过程中可能会遇到的问题以及排查思路，主要分为以下几个步骤：首先，需要对 iMC 服务器以及 iMC 的安装部署进行合规检查，确保安装环境符合规范；其次，需要对 AC 以及 AP 状态的检查，查看 AC 以及 AP 是否可以正常添加以及显示；再次，要查看所购买或者试用的 WSM 的业务功能授权，保证现有的 License 满足需求；最后，对 WSM 各业务功能的检查，其中包括无线定位功能的检查，移动终端用户的检查以及节能策略的检查。

2. 流程图相关操作说明

(1) iMC 服务器相关检查

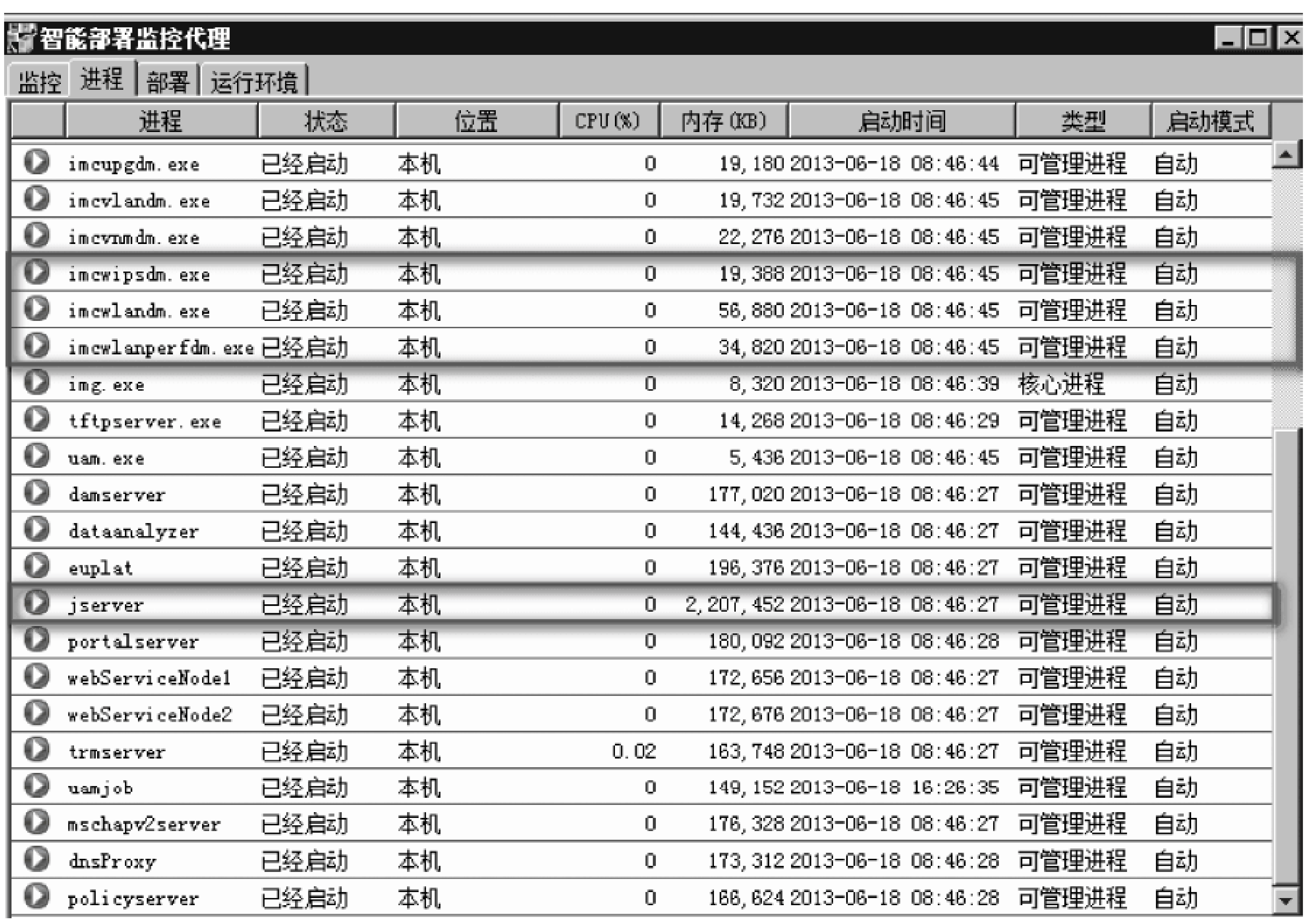
在使用 WSM 前，需要对 iMC 服务器的部署情况、运行情况以及相关配置等做一个完整的、规范的检查，确保服务器符合 iMC 安装指导的要求。主要注意以下几点。

① 服务器是否符合《智能管理中心(iMC)部署和硬件配置方案》，需要重点检查以下两点。

(a) WSM 服务器是否符合安装以及运行的要求，主要查看服务器物理内存以及 cpu 的占用情况。

(b) 在管理 AP 数目较多的大规模应用场景下，WSM 服务器是否进行了合理的分布式部署。

② 查看 WSM 以及前台 Web 页面的主进程是否正常启动，如图 8-393 所示。



智能部署监控代理

监控 | 进程 | 部署 | 运行环境

进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
imcupgdm.exe	已经启动	本机	0	19,180	2013-06-18 08:46:44	可管理进程	自动
imcvlandm.exe	已经启动	本机	0	19,732	2013-06-18 08:46:45	可管理进程	自动
imcvmmdm.exe	已经启动	本机	0	22,276	2013-06-18 08:46:45	可管理进程	自动
imcwipsdm.exe	已经启动	本机	0	19,388	2013-06-18 08:46:45	可管理进程	自动
imcwlandm.exe	已经启动	本机	0	56,880	2013-06-18 08:46:45	可管理进程	自动
imcwlanperfdm.exe	已经启动	本机	0	34,820	2013-06-18 08:46:45	可管理进程	自动
img.exe	已经启动	本机	0	8,320	2013-06-18 08:46:39	核心进程	自动
tftpserver.exe	已经启动	本机	0	14,268	2013-06-18 08:46:29	可管理进程	自动
uam.exe	已经启动	本机	0	5,436	2013-06-18 08:46:45	可管理进程	自动
damserver	已经启动	本机	0	177,020	2013-06-18 08:46:27	可管理进程	自动
dataanalyzer	已经启动	本机	0	144,436	2013-06-18 08:46:27	可管理进程	自动
euplat	已经启动	本机	0	196,376	2013-06-18 08:46:27	可管理进程	自动
jserver	已经启动	本机	0	2,207,452	2013-06-18 08:46:27	可管理进程	自动
portalserver	已经启动	本机	0	180,092	2013-06-18 08:46:28	可管理进程	自动
webServiceNode1	已经启动	本机	0	172,656	2013-06-18 08:46:27	可管理进程	自动
webServiceNode2	已经启动	本机	0	172,676	2013-06-18 08:46:27	可管理进程	自动
trmserver	已经启动	本机	0.02	163,748	2013-06-18 08:46:27	可管理进程	自动
uamjob	已经启动	本机	0	149,152	2013-06-18 16:26:35	可管理进程	自动
mschapv2server	已经启动	本机	0	176,328	2013-06-18 08:46:27	可管理进程	自动
dnsProxy	已经启动	本机	0	173,312	2013-06-18 08:46:28	可管理进程	自动
policyserver	已经启动	本机	0	166,624	2013-06-18 08:46:28	可管理进程	自动

图 8-393　Web 页面进程启动情况

说明：

(a) imcwlandm.exe 以及 imcwlanperfdm.exe 为 WSM 的主进程，只要正常安装部署了 WSM 组件，肯定会有以上两个进程。

(b) imcwipsdm.exe 为 WSM 中 WIPS 功能的进程，WIPS 需要购买单独的 License（包括设备上的 License），注册成功以后启动 iMC，可以正常看见此进程。

(c) jserver 进程为 iMC 前台 Web 页面的主进程，若要正常浏览网页，则要保证它正常启动。

③ 查看 iMC 服务器与 AC 是否可达，SNMP 参数是否正确：判断是否可达只要在 iMC 服务器 ping AC 可达即可验证；查验 SNMP 参数配置是否正确则需要对比设备以及 iMC 的相关信息，在设备列表中单击“设备”标签，进入设备详细信息页面，如图 8-394 所示。



图 8-394　设备详细信息页面

如果在设备以及 iMC 上正确配置了只读团体字，那么设备详细信息页面的数据都可以正常显示，读写团体字需要通过查看设备 SNMP 的具体配置以及 iMC 侧 SNMP 参数（模板）的配置来确认。单击配置中的“修改 SNMP 参数”，进入配置页面后，由于读写团体字不可见，需要手动检查、修改 SNMP 读写团体字并与设备保持一致，如图 8-395 所示。



图 8-395　SNMP 参数设置

在保证了以上几点之后，就可以正常使用 WSM 资源管理功能了。

(2) AC 及 AP 状态检查

进入 WSM 资源管理中以后，需要检查 AC 以及 AP 的状态，正常状况下，添加进 iMC 的 AC 会被自动识别为无线设备并添加至 WSM 资源管理中，如图 8-396 所示。



图 8-396　AC 以及 AP 状态

如果 AC 已经按照添加设备的流程增加进 iMC 后，在 WSM 资源管理的无线控制器里却无法看到此设备，可以按照如下步骤排查：首先，检查 iMC 以及 AC 的版本信息，确保 iMC 支持此 AC(可以查看 iMC 的版本说明书)；然后，通过添加设备或同步设备时的抓包检查 SNMP 是否超时。目前已知的几个主要问题以及解决方法如下：①AC 以及 iMC 版本问题。如果是 AC 版本较老，可以将设备的软件版本升级、更新；而 iMC 5.2 E0401 版本存在 MIB 兼容问题，需要升级至 5.2 E0401H03 及以上版本才可，而 5.2 以前版本不存在此问题。对于 MIB 风格问题，如果网络中设备数目较少，还可以考虑将设备的 MIB-Style 改为 New 风格的 MIB，若设备数量大，还是考虑升级 iMC 版本。②乱码问题。在确定某台 AC 或 AP 命名出现乱码问题以后，删除并更新设备配置信息，重新添加或同步 AC 以后，问题可以得到解决。此问题的根本解决办法还是在开局的时候，对整体无线网络进行规范的配置，以避免后续不必要的麻烦才是上上策。③SNMP 问题。最好先排查网络原因，保证 iMC 服务器与 AC 之间的网络通断正常；SNMP 超时的问题，若网络正常，则需要在 iMC 服务器侧将 SNMP 超时时间调长，一般先调至 30 秒(或者调整至更合适的时间)，保证 iMC 及时收到返回的 SNMP 报文，这种问题主要是由于网络延迟造成，具体可以查看 KMS 案例《iMC 添加 AC 后在 WSM 组件无法看到 AC 以及同步 AC 信息失败的解决办法》。

(3) WSM License 功能授权检查

WSM 和 iMC 的其他业务组件一样，有着严格的 License 控制策略，在使用 WSM 前，需要确认购买或试用的 License 满足需求。在进入 iMC 以后，单击页面右上角“关于”按钮，可以查看注册的无线 License 信息如图 8-397 所示。

由于频谱防护、网络评估为 WSM 5.1-E0302 版本才首次具有的功能，所以如果购买并注册了 License 但是在关于中看不到相关功能，首先需要确定 WSM 版本信息；其次确定 License 注册完成是否重启了 iMC。

组件信息 标准版 将于2013年8月12日失效。

组件	版本	许可数量	已使用数量	失效日期
无线业务管理	iMC WSM 5.2 (E0402P05)	允许管理最大AP数：2100	4	2013-8-12
		定位功能	--	2013-8-12
		实时定位最大节点数：150		2013-8-12
		网络评估	--	2013-8-12
		频谱防护	--	2013-8-12
		WIPS允许管理最大Sensor数：550	0	2013-8-12

图 8-397　注册无线 License 信息

还有，在 WSM 组件中 AC 和 FAT AP 占用 iMC PLAT 的 License，而 FIT AP 需要使用相应节点的 License，节点数是由 AC 上配置的 AP 模板决定的，如果客户的节点数目超出了，需要在 AC 上删除多余的模板或购买 License 扩容激活。无线定位功能 License 包括了基于 AP 的非实时定位、基于 iNode 客户端的实时定位，其中基于 iNode 客户端的实时定位也需要有相应的节点。

（4）无线定位功能的检查

无线定位功能的原理：通过指纹采样算法，在大于等于 3 台 AP 的无线环境中设置采样点采集无线信号衰减以及距离信息（存入后台数据库），当终端接入 AP 以后，通过 AP 主动扫描信道扫描信道（基于 AP 的非实时定位）或通过 iNode 客户端发送实时通信报文（基于 iNode 的实时定位）来对接入终端、用户进行拓扑定位展示。

正常情况下，设置完采样点进行采样以后，单击“移动终端”的定位，这时会将终端定位在无线位置视图拓扑中（定位在采样点上），如果定位失败，则需要检查移动终端是否设置为采样点以及采样情况，首先检查 WSM 资源管理的移动终端中是否将在线的移动终端 MAC 设置为采样用户，如图 8-398 所示。



图 8-398　采样用户

然后检查在位置视图中采样点的间隔是否符合要求（5～10 米）以及选择终端 MAC 地址是否正确，如图 8-399 所示。



图 8-399　选择 MAC

最后检查采样点是否正确采样结束(10 分钟左右,具体看网络环境)。

(5) 无线终端用户信息检查

在 WSM 资源管理的“移动终端用户”模块,正常情况下如果手动增加了用户信息,可以查看接入的移动用户以及实时监控等信息,如图 8-400 所示。

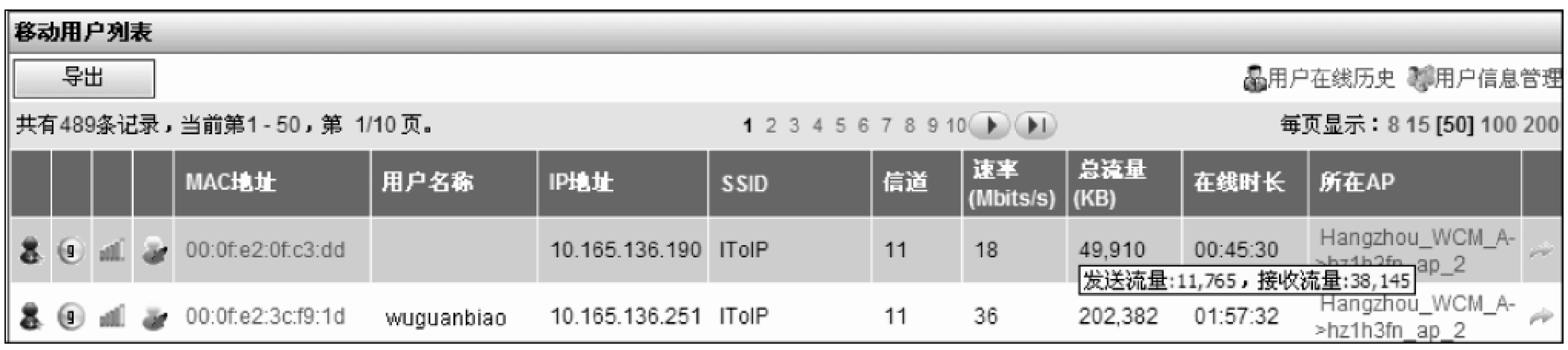


图 8-400　移动用户列表

如果在移动终端中查看用户名称为空,则有以下几种原因:一是没有在无线设备配置 802.1x 认证;二是没有认证也没有手动增加用户信息;三是有 UAM 服务器但是没有相应的配置去同步 UAM 信息。

移动终端列表用户名称按以下方式获取。

① 如果网络管理员在无线设备中配置 802.1x 认证方式接入的无线网络,无线设备可以获取到用户在 802.1x 认证中使用的用户名,移动终端列表中用户名称显示设备上获取的用户名称。

② 操作员在终端信息管理中增加移动终端 MAC 和用户名称对应关系后,移动终端列表中用户名称显示终端信息管理中的用户名。如果能够通过方式①获取用户名,则该方式无效。

③ 如果 UAM 组件中存在该用户的 IP 地址和用户名绑定的情况,则移动终端列表中用户名称显示 UAM 中的用户名。如果能通过方式①、②获取用户名,则该方式无效。

④ 如果 UAM 组件中存在该用户的 MAC 地址和用户名绑定的情况,则移动终端列表中用户名称显示 UAM 中的用户名。如果能通过方式①、②、③获取用户名,则该方式无效。

⑤ 如果 UAM 组件的在线终端表中存在该无线用户时,则移动终端列表中用户名称显示 UAM 中在线用户表中的用户名。如果能通过方式①、②、③、④获取用户名,则该方式无效。

例如:有移动终端通过 802.1x 认证方式接入无线网络,认证时使用的用户名称是 A,则移动终端列表名称显示 A。此时如果通过终端信息管理功能增加一条该终端 MAC 和用户名的绑定关系,如用户名为 B,则移动终端列表用户名称还是显示 A,如果用户下线后,再次接入时不通过 802.1x 认证方式接入无线网络,则用户名称显示 B。简而言之:通过 802.1x 认证

上线,则使用认证时的用户名,下线则使用自定义的用户名。

如果想要看到用户名称,有三种办法:一是在无线设备配置 802.1x 认证,这时 WSM 会获取通过认证的用户名称;二是手动添加用户信息,将 MAC 和用户信息相互绑定;三是需要与 UAM 服务器联动,将 UAM 服务器上的用户信息同步至 WSM 资源管理中,同步以后就可以看见移动终端用户的相关信息,可以单击 WSM 中的"配置管理",然后选择"UAM 服务参数配置",最后对 UAM 服务器 IP 地址、登录端口、登录名和密码进行配置,如图 8-401 所示。



图 8-401 UAM 服务参数配置

单击"确定"按钮以后,就可以联动 UAM 服务器对终端用户名进行同步了。

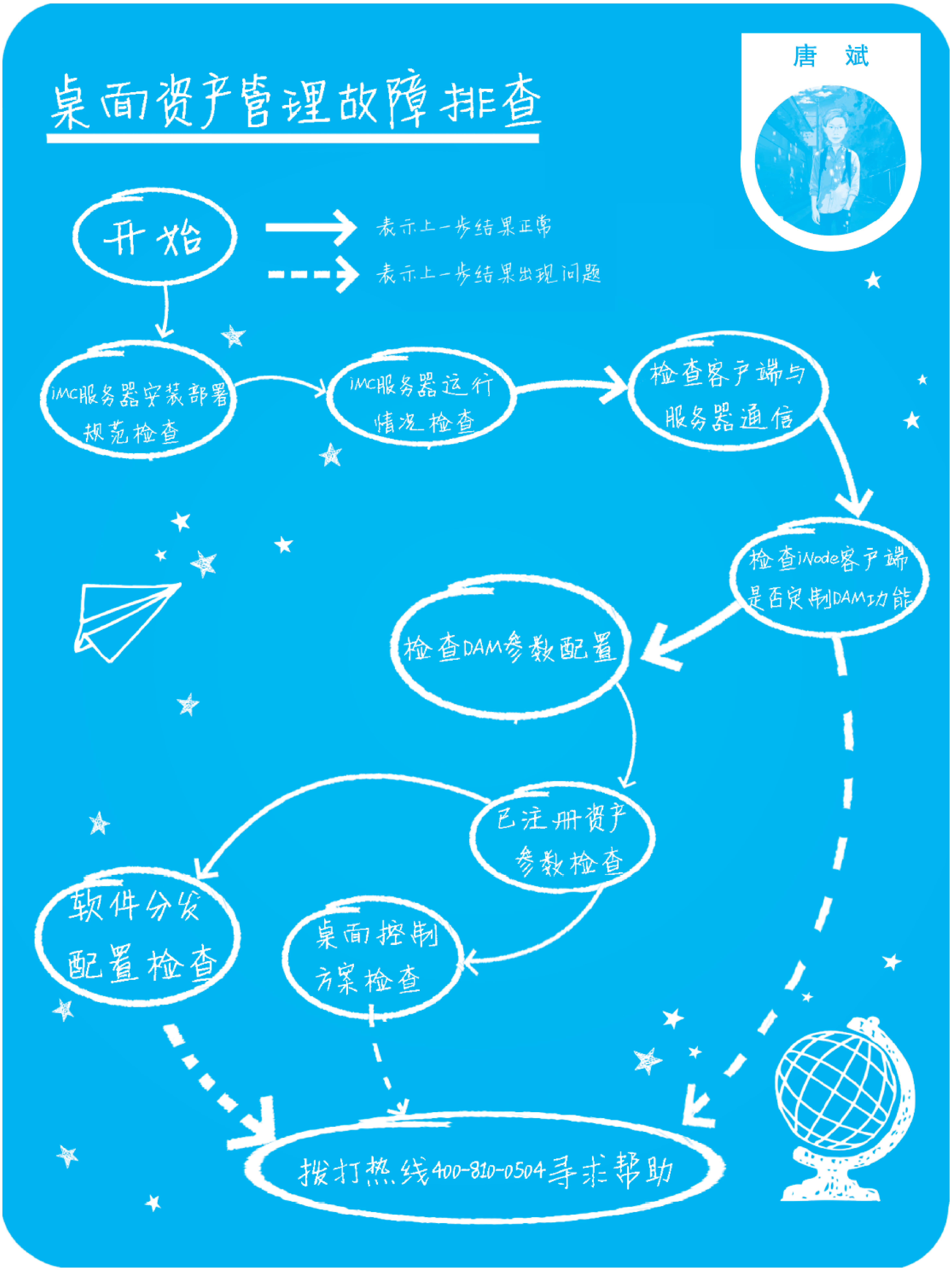
(6) 节能策略检查

节能策略的配置如图 8-402 所示。



图 8-402 节能策略配置

在使用 WSM 节能策略管理的时候,下发一些策略可能会出现不成功的情况。比如,在下发 AP 启动停止时,到达指定时间,发现策略未生效,这时需要检查 AP 是否支持 POE 供电,支持的设备才能正确下发。



桌面资产管理故障排查
唐 斌
开始
表示上一步结果正常
表示上一步结果出现问题
iMC服务器安装部署规范检查
iMC服务器运行情况检查
检查客户端与服务器通信
检查iNode客户端是否定制DAM功能
检查DAM参数配置
已注册资产参数检查
桌面控制方案检查
软件分发配置检查
拨打热线400-810-0504寻求帮助

1. 开始

桌面资产管理通过 iNode 客户端与 iMC DAM 组件通信建立连接，进行注册资产。针对已注册的桌面资产生效桌面控制方案和软件分发策略。

排错思路为：首先，检查服务器各组件部署情况和运行状态，查看 DAM 相关端口的使用状况；其次，检查客户端定制和与服务器之间通信的情况；最后，在 DAM 配置台中检查具体配置参数。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范性检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案 》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”各组件是否是已部署的状态。

需要关注的组件有用户管理相关组件，其状态都应为“已部署”。

查看 iMC 安装部署桌面资产管理组件如图 8-403 所示。两个组件必须是“已部署”。



图 8-403 组件部署情况

(2) iMC 服务器运行情况检查

① 查看部署监控代中 damserver 的进程状态，正常情况下该进程状态为“已经启动”。对于桌面资产管理和代理服务器分布式安装会有进程 damproxy。图 8-404 所示为集中式部署时 DAM 的进程截图。

② 检查服务器上端口 8015、8027、9023、9025、9027、9029 的使用情况。

在命令提示符中输入 netstat -aon|findstr :9029 查看使用 9029 端口的进程的 PID。输入 netstat -aon|findstr :14352，如图 8-405 所示。回车显示的是该 PID 的进程使用的端口有哪

些。正常显示如图 8-405 所示。另外,在任务管理器中对应 PID 的进程应该为 iMC 的进程,显示为 java. exe 或 javaw. exe。若显示不正常,请排查缺失端口是否让非 iMC 进程占用,并重启 damserver 的进程。

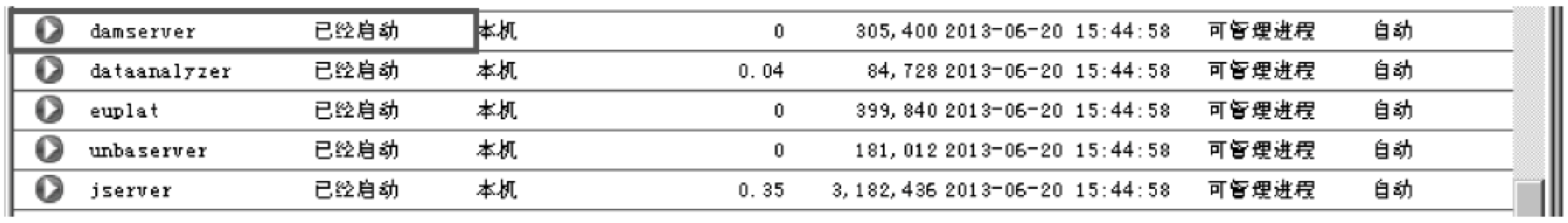


图 8-404　集中式部署时 DAM 进程图



图 8-405　端口使用情况

说明:

(a) Windows 操作系统中,通过

netstat-aon|*findstr* :端口号

命令来显示某一端口的监听状态及其对应的进程 PID,如图 8-406 所示。

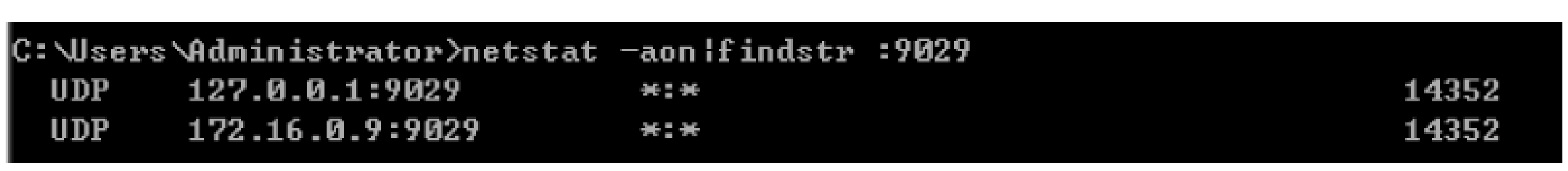


图 8-406　命令显示

其中第一列 UDP 所指监听的协议;第二列所指监听的服务器的 IP 和端口号;第三列 *:* 代表此行信息为监听状态;最后一列 14352 代表此协议监听的进程 PID。查到端口所对应的进程 PID 后,请查看 Windows 任务管理器,通常 java 或 javaw 就是 iMC 各组件使用的进程。

(b) 端口介绍

8015:DAM 服务器侦听停止命令端口。

8017:DAM 服务器侦听配置台发送的日志级别更新报文端口。

9023:DAM 服务器监听配置台通知报文和策略服务器回应报文。

9025:DAM 服务器与 DAM 代理服务器通信时,DAM 服务器侧端口。

9027：DAM 服务器与 DAM 代理服务器通信时，DAM 代理服务器侧端口。

9029：DAM 代理服务器监听客户端请求报文端口，iNode 向此端口发送 DAM 各种请求报文。

(3) 检查客户端与服务器通信

检查客户端与服务器网络连通性。可通过 ping 命令检查客户端与服务器之间网络是否可达，如图 8-407 所示。

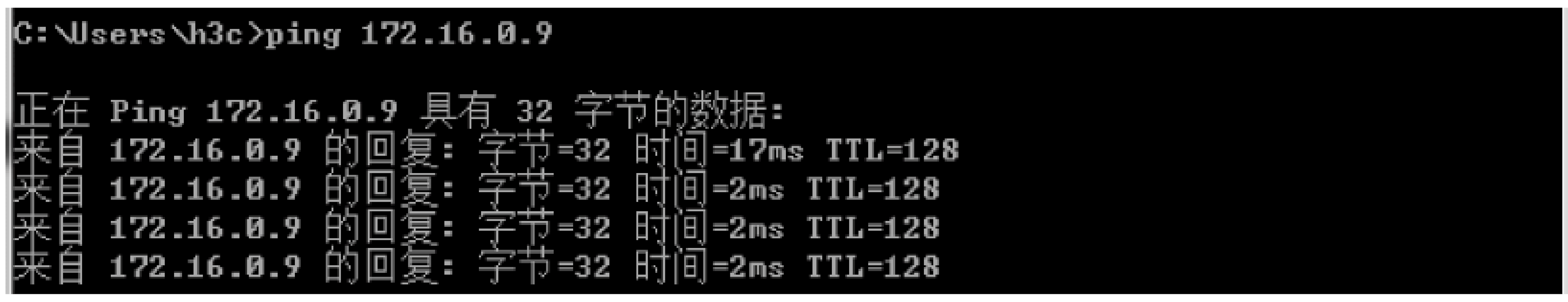


图 8-407　检查客户端与服务器通信

(4) 检查 iNode 客户端是否定制 DAM 功能

① 查看 iNode 客户端是否定制了 DAM 功能，查看方法如图 8-408 所示。



图 8-408　定制的 DAM 功能

② 检查终端任务管理器中的进程 DamAgent.exe 是否正常运行，具体如图 8-409 所示。



图 8-409　进程正常运行

(5) 检查 DAM 参数配置

进入 iMC 管理界面，依次单击“业务”→“桌面资产管理”→“业务参数配置”→“系统参数配置”命令。对于禁用资产自动编号的默认系统配置如图 8-410 所示。

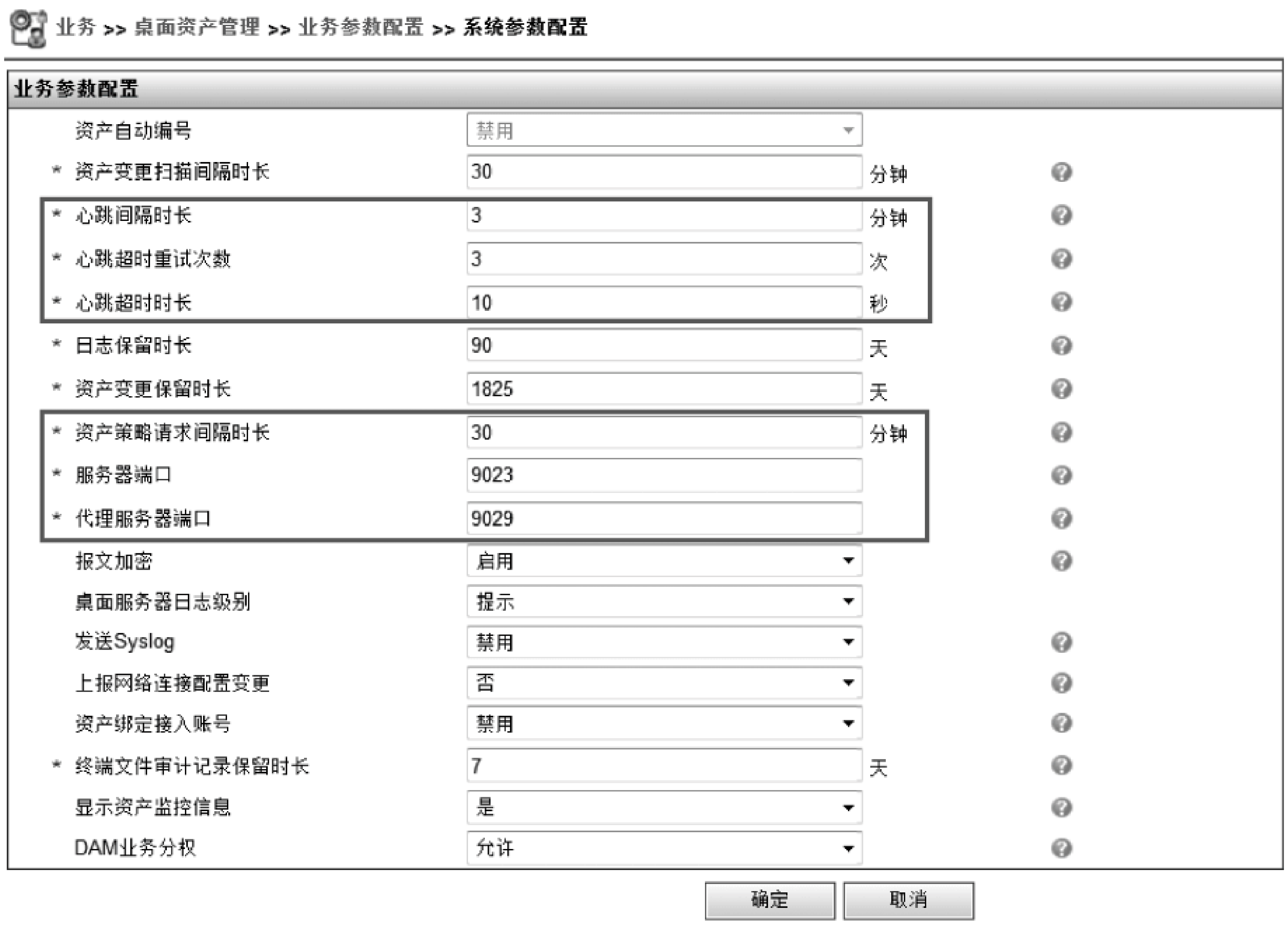


图 8-410　禁用资产自动编号默认系统配置

各主要参数检查及调整方法如下。

① 心跳时间设置是否合适的检查方法。在终端与服务器实际可达的前提下，终端 iNode“信息”→“桌面资产管理客户端连接注册信息”中，若经常显示“已注册未连接”，表示终端与 DAM 服务器常处于通信不畅的状态，可以增加“心跳超时重试次数”，增加“心跳超时时长”。

② 资产变更扫描间隔时长的检查方法。在终端上安装卸载软件，造成资产变更的现象。在单击 iMC“业务”→“桌面资产管理”→“资产软件变更”命令后查看变更记录的更新时间。默认为 30 分钟，测试时可以将参数改得短一下，比较邻近变更的时间是否为设置的参数范围内。

③ 上报网络连接配置变更的检查方法。因为网络配置变更划入软件变更中，所以可与资产变更扫描间隔时长的检查同时进行。资产变更扫描间隔时长设为 3 分钟时，效果如图 8-411 所示。



图 8-411　变更的检查

④ 资产绑定接入账号的检查方法。对于资产 T09445 来说，它绑定的用户是 tom。若非 tom 的用户上线，iNode 上注册资产 T09445 是不会成功的。提示如图 8-412 所示。

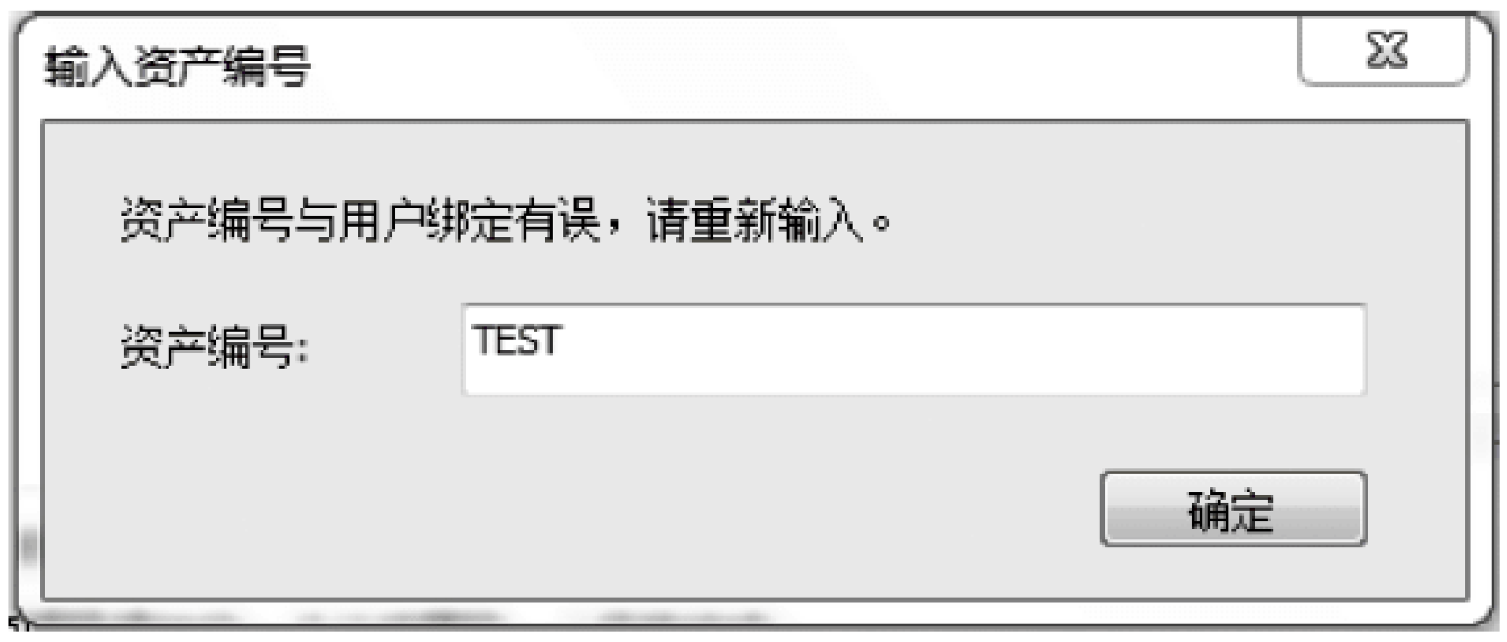


图 8-412 “输入资产编号”对话框

说明：

(a) 资产变更扫描间隔时长：客户端通过定时扫描资产信息(除磁盘分区以外)的方式来发现资产软硬件是否变更，本参数设置客户端定时扫描时间间隔。磁盘分区仅在客户端启动时扫描一次，防止频繁扫描损耗磁盘。

(b) 日志保留时长：外设、打印机和 USB 三种监控日志在数据库中保留的时长。系统会在每天凌晨清除超过保留时长的监控日志。

(c) 资产变更保留时长：资产软硬件变更在数据库中保留的时长。系统会在每天凌晨清除超过保留时长的资产软硬件变更。

(d) 终端文件审计记录保留时长：终端文件审计记录在数据库中保留的时长，超过该时长的审计记录将会在每天凌晨自动删除。

(e) 其他参数请查看联机帮助

(6) 已注册资产参数检查

查看具体资产的状态、编号、责任人等信息。

桌面资产的状态有 3 种：“未管理”“离线”“在线”。已注册的资产根据是否上线，显示为“离线”或“在线”状态。未注册的资产显示为“未管理”。

单击桌面资产的编号，可查看资产完整信息，如图 8-413 所示。



图 8-413 查看资产完整信息

(7) 桌面控制方案检查

① 桌面控制方案中控制策略有三类：外设管理策略、绿色节能策略、监控告警策略，如图 8-414 所示。可单击“业务”→“桌面资产管理”→“桌面监控策略管理”命令，查看具体策略内容，如图 8-415 所示。

② 确定资产已引用相应的桌面控制方案。资产下发控制方案的方法有两种：对资产分组配置桌面资产控制方案，或针对单个资产选择桌面资产控制方案。其中两者中的控制方案不同时，单个资产中的控制方案优先生效，如图 8-416 所示。



图 8-414　三类控制策略



图 8-415　具体策略内容



图 8-416　资产的桌面控制方案

（8）软件分发配置检查

软件分发主要对分发服务器和分发的任务进行检查，包括“软件分发服务器”和“软件分发任务”的检查。

① 软件分发服务器。

第一，确保软件服务器可达。

第二，确保软件服务器上的端口可用。

第三,确保相应的服务已启用,包括 FTP、Http、共享文件等方式。

② 软件分发任务。

分发任务的检查方法。以 FTP 方式分发的情况为例,在分发任务配置界面,单击“测试方法”,如图 8-417 所示。



图 8-417 分发任务检查

根据弹出的提示页面进行测试。方法即在浏览器中下载路径输入 URL,输入用户名密码,打开或下载文件,以验证配置是否成功,如图 8-418 所示。

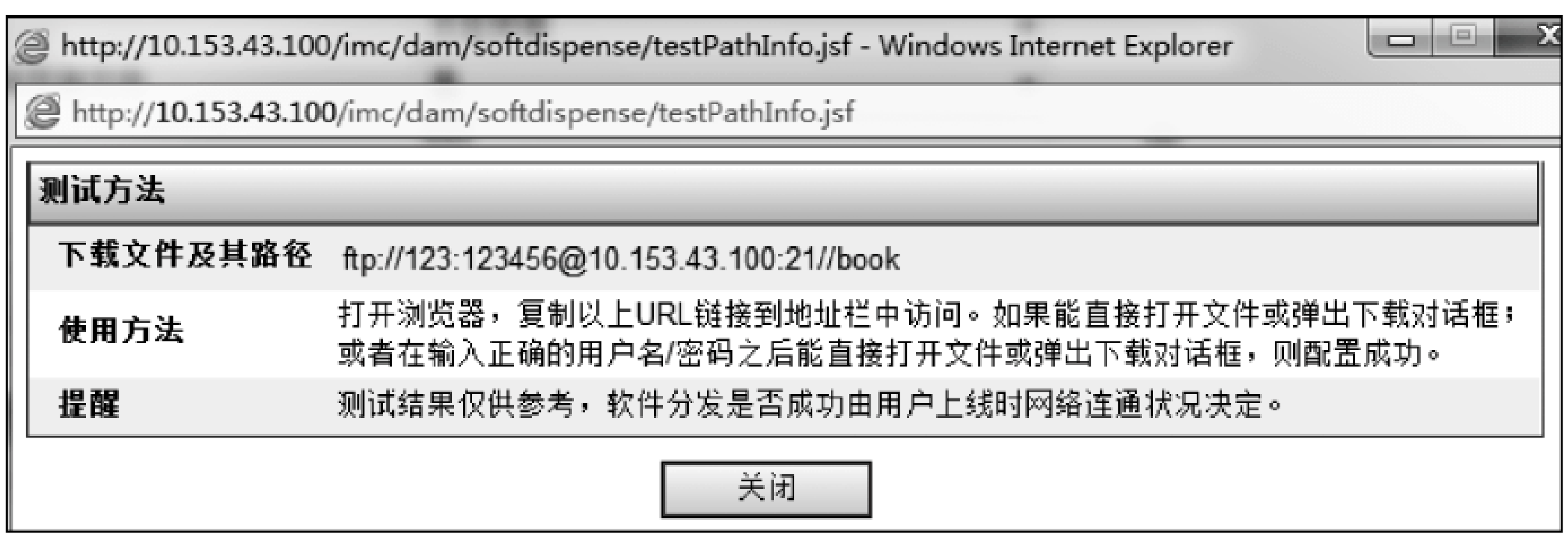


图 8-418 测试方法


DAM软件分发故障排查
表示上一步结果正常
表示上一步结果出现问题
常 杉
开始
是否全局故障
全局故障优先排查服务器侧
个别用户故障优先排查客户端侧
服务器操作是否正常
iMC服务器安装部署规范检查
iMC服务器运行情况检查
DAM服务器和DAM客户端连通性检查
DAM客户端在线状态检查
DAM服务器配置检查
第三方文件服务器可用性检查
DAM客户端运行状况检查
DAM客户端连通性检查
DAM客户端在线状态检查
第三方文件服务器可用性检查
DAM客户端下载软件MD5检查
拨打热线
400-810-0504
寻求帮助

1. 开始

DAM 软件分发功能简介：DAM 服务器通 Http、FTP、文件服务器方式给已在线 DAM 客户端下发软件，客户端下载完成后，进行安装等操作将软件部署在客户端 PC 中。

DAM 软件分发功能排错定位思路：功能分为三大主体，即 iMC DAM 服务器、iNode DAM 客户端、文件服务器。对于不同现象，排查不同主体以得到快速解决问题的目的。

本文举例组网如图 8-419 所示。

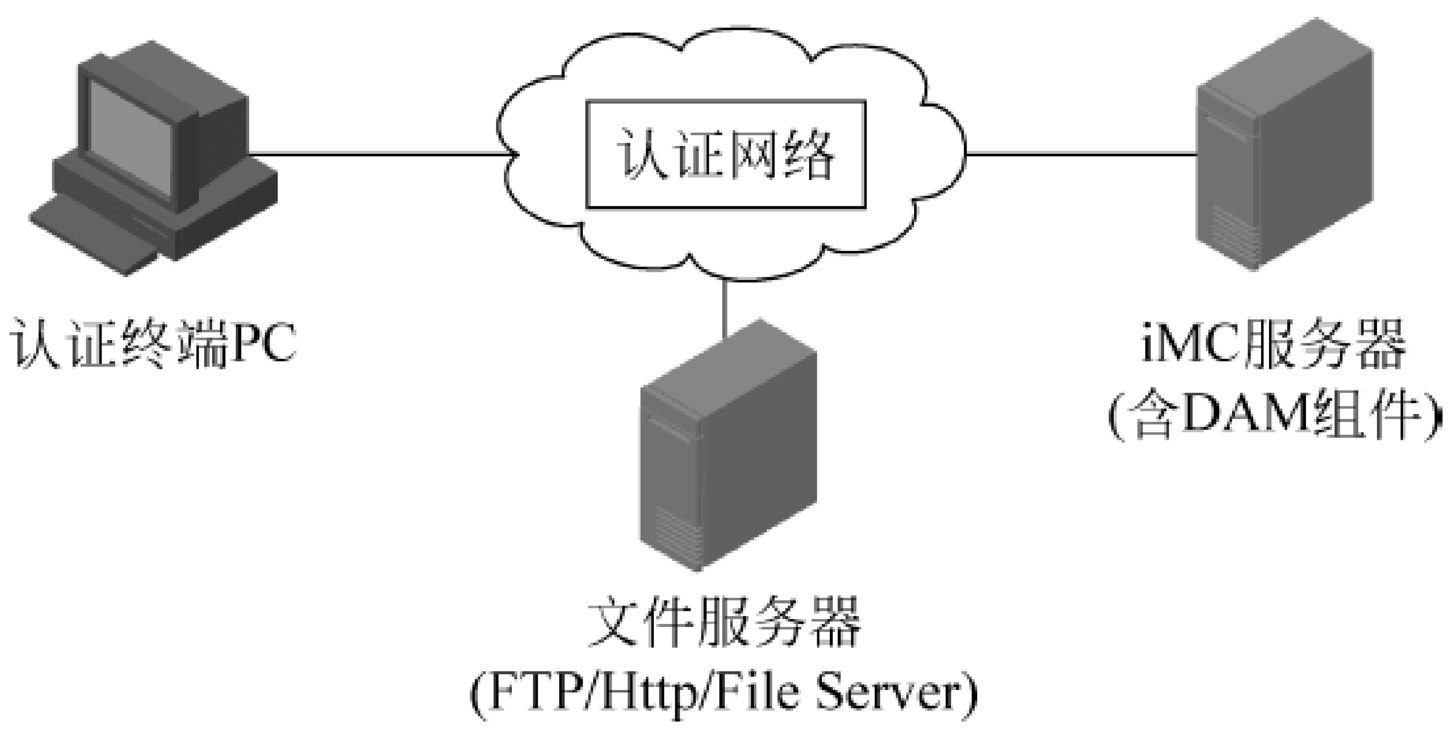


图 4-419　组网举例

由于此功能实现在认证成功之后，故不给出认证网络规划等相关配置。

2. 流程图相关操作说明

通过现象判断出现的问题是否是全局存在，区分对待不同现象进行排查。

(1) 对于出现在个别终端上的问题优先从客户端角度去排查

常见的问题现象有客户端 DAM 服务没有启动，客户端未连接服务器，下载的软件安装包文件错误等。

(2) DAM 客户端运行状况检查

① 任务管理器中是否有 DamAgent. exe 进程运行，如图 8-420 所示。



图 8-420　DamAgent. exe 运行情况

② 检查 iNode DAM 服务项是否正常启动。

运行 services. msc，在服务配置中查找 iNode DAM Agent 服务，并检查其状态，如图 8-421 所示。

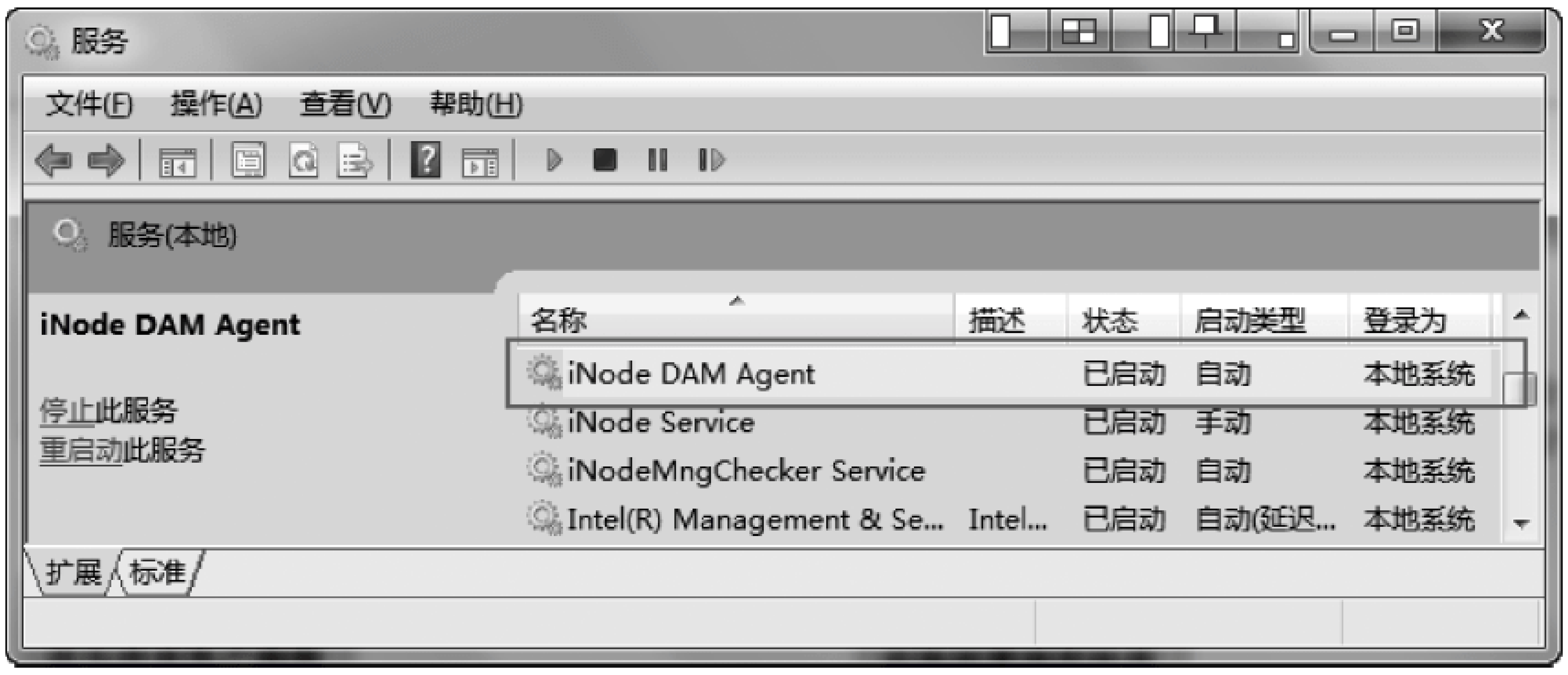


图 8-421 iNode DAM Agent 服务

（3）DAM 客户端连通性检查

从 DAM 客户端侧分别 ping 测试 DAM 服务器、策略中配置的文件服务器的连通性，在网络上、服务器上不禁止 ping 的情况下，要确保服务器均可达。如有可达性的问题，需要排查网络。

（4）DAM 客户端在线状态检查

在 iNode 客户端中单击菜单项“信息”→“桌面资产管理客户端连接注册信息”命令，如图 8-422 所示。

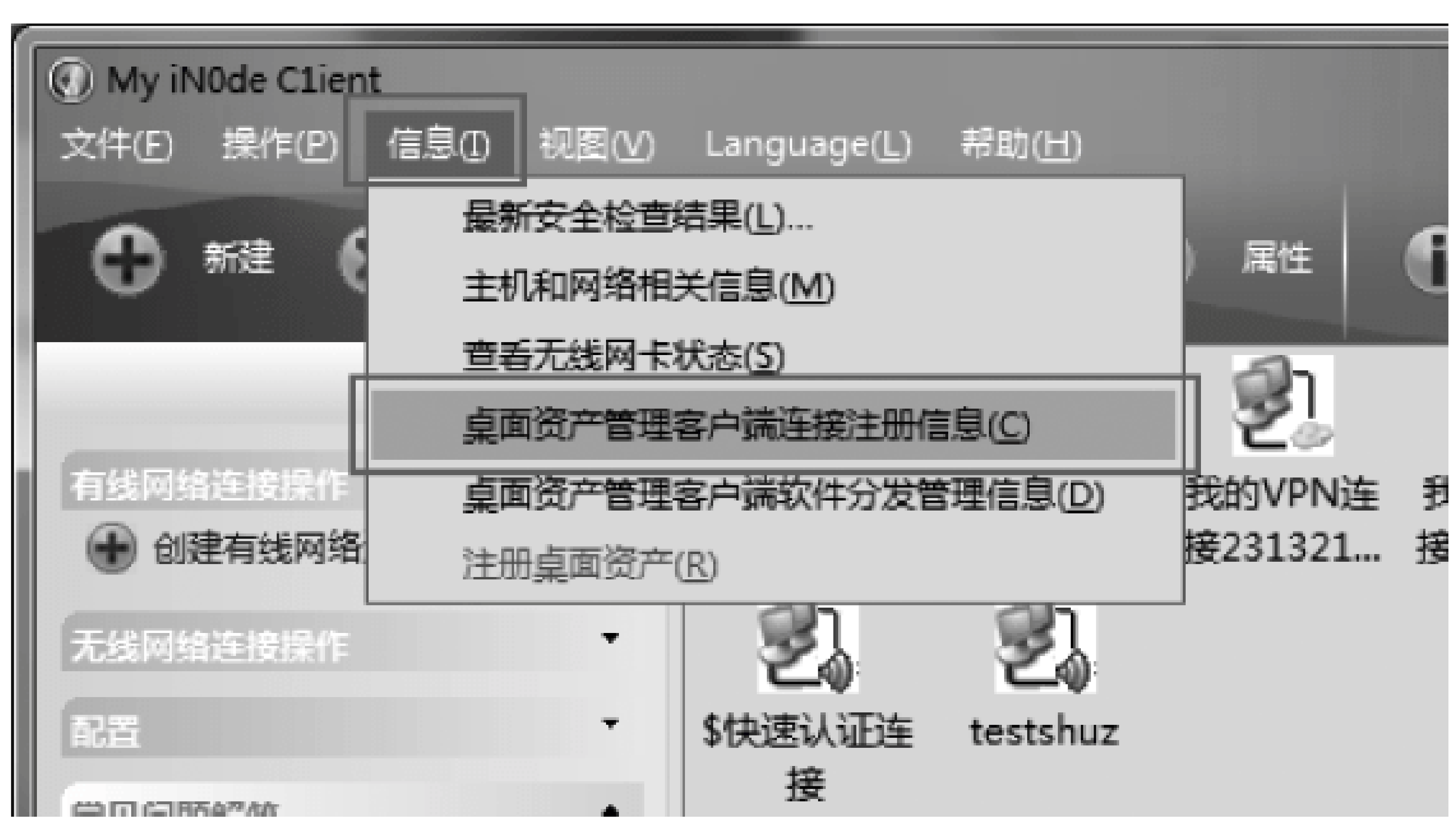


图 8-422 “桌面资产管理客户端连接注册信息”

查看“桌面资产管理客户端”窗口中各状态是否是“正在运行”“已连接”“已注册”。如有其他状态，请先参考云图《桌面资产管理故障排查》将客户端状态修正，如图 8-423 所示。

（5）第三方文件服务器可用性检查

根据不同服务器类型 Http、FTP、文件服务器分别在客户端侧检测器可用性。

① Http 进行软件分发，可使用 IE 浏览器进行 URL 的直接下载的（多余）操作，查看是否可以正常下载到要分发的软件，如图 8-424 所示。

② 对于 FTP 服务器，可使用命令行中的 FTP 命令将服务器上的文件下载到本机进行测试，如图 8-425 所示。

③ 文件服务器进行软件分发，直接使用 Windows 资源管理器测试文件是否可以正常拷贝到本地，如图 8-426 所示。



图 8-423　“桌面资产管理客户端状态”

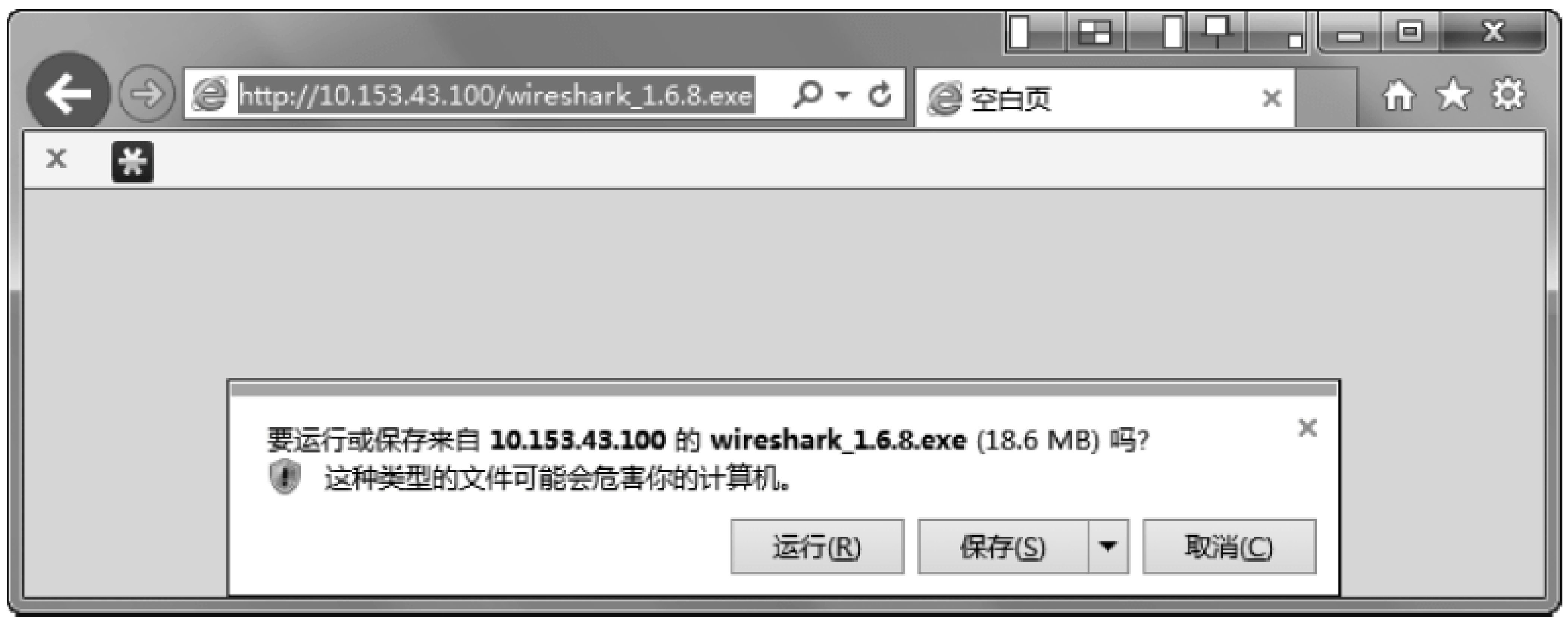


图 8-424　Http 软件分发

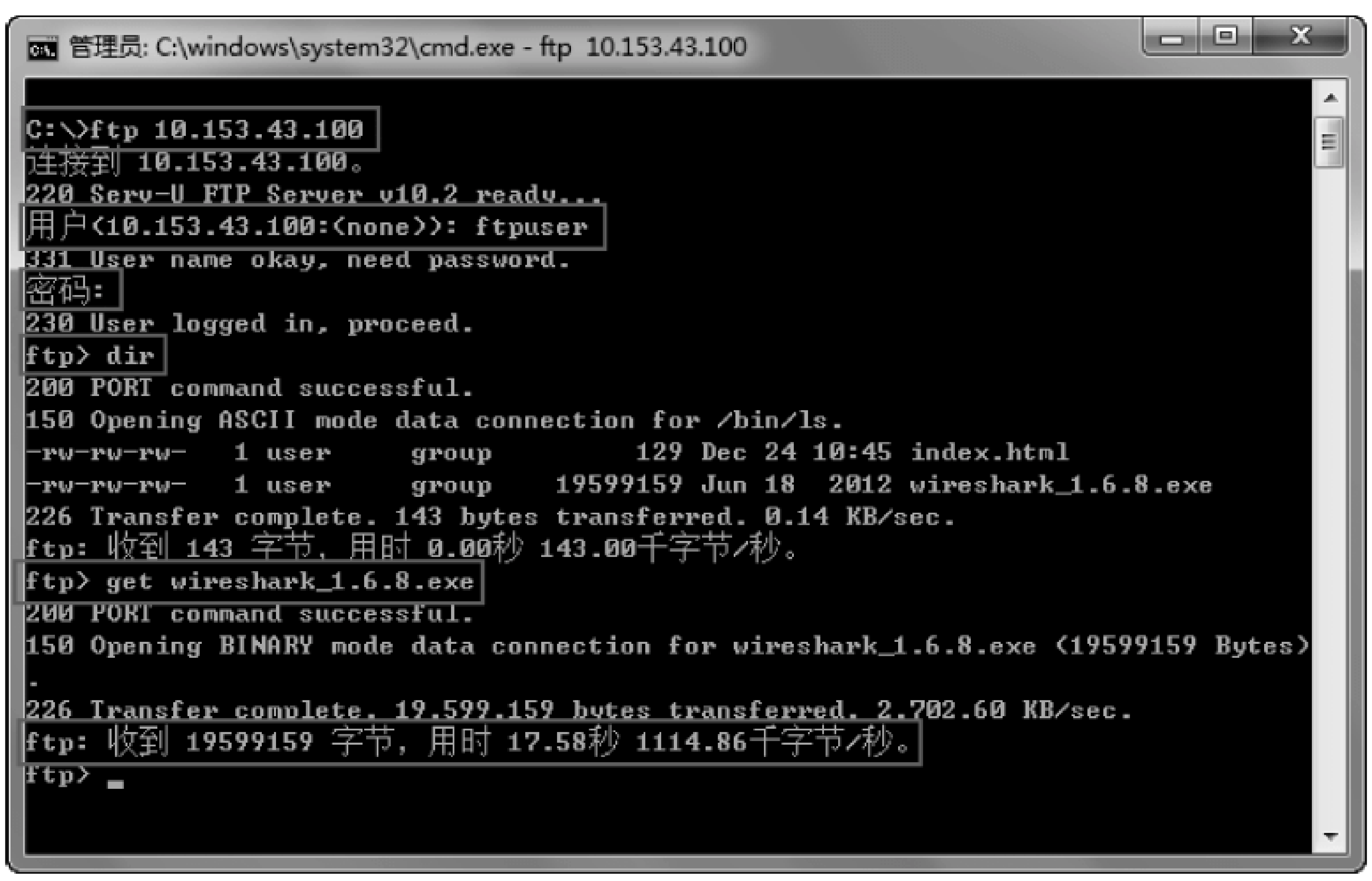


图 8-425　FTP 命令



图 8-426　文件服务器软件分发

④ 如果以上软件出现不能下载的情况，请先将下载功能调通。

(6) DAM 客户端下载软件 MD5 检查

可自行下载 MD5 校验软件，将所下载的文件和服务器上的文件进行 MD5 值的哈希校验比较。DAM 客户端自动下载的文件路径在“C:\iNode DAM Agent\(十六进制字符串)\SoftDlvrMng\”路径下，可打开该目录找到分发软件文件。

举例：通过 DM5 值计算结果不同比较出两个文件不相同，如图 8-427 所示。



图 8-427　DM5 值计算不同比较两个文件不同

(7) 全局故障优先排查服务器侧

若全部客户端都存在问题，建议先从服务器端着手排查问题。首先请访问 iMC 服务器 Web 配置界面和服务器本地，查看其操作是否有严重卡顿等不正常操作现象，如有，需要先检查 iMC 服务器配置规范性和 iMC 服务器运行情况。

(8) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查服务器侧问题时首先要确认服务器软硬件配置情况是否符合要求。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器对应业务量的配置需求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”各组件是否是已部署的状态。

需要关注的组件有“用户接入管理”和“Portal 服务器”，其状态都应为“已部署”，如图 8-428 所示。

(9) iMC 服务器运行情况检查

查看“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程，各进程是否正常为



图 8-428　组件部署情况

“已经启动”。

① 打开部署监控代理，查看 damserver 进程是否正常启动。由于 DAM 服务器需要在认证(不一定认证)结束后发起 DAM 相关操作，所以也需要确认 uam.exe、policyserver 等认证相关进程是否正常，更具体的排查方法请参考相关云图文档，如图 8-429 所示。

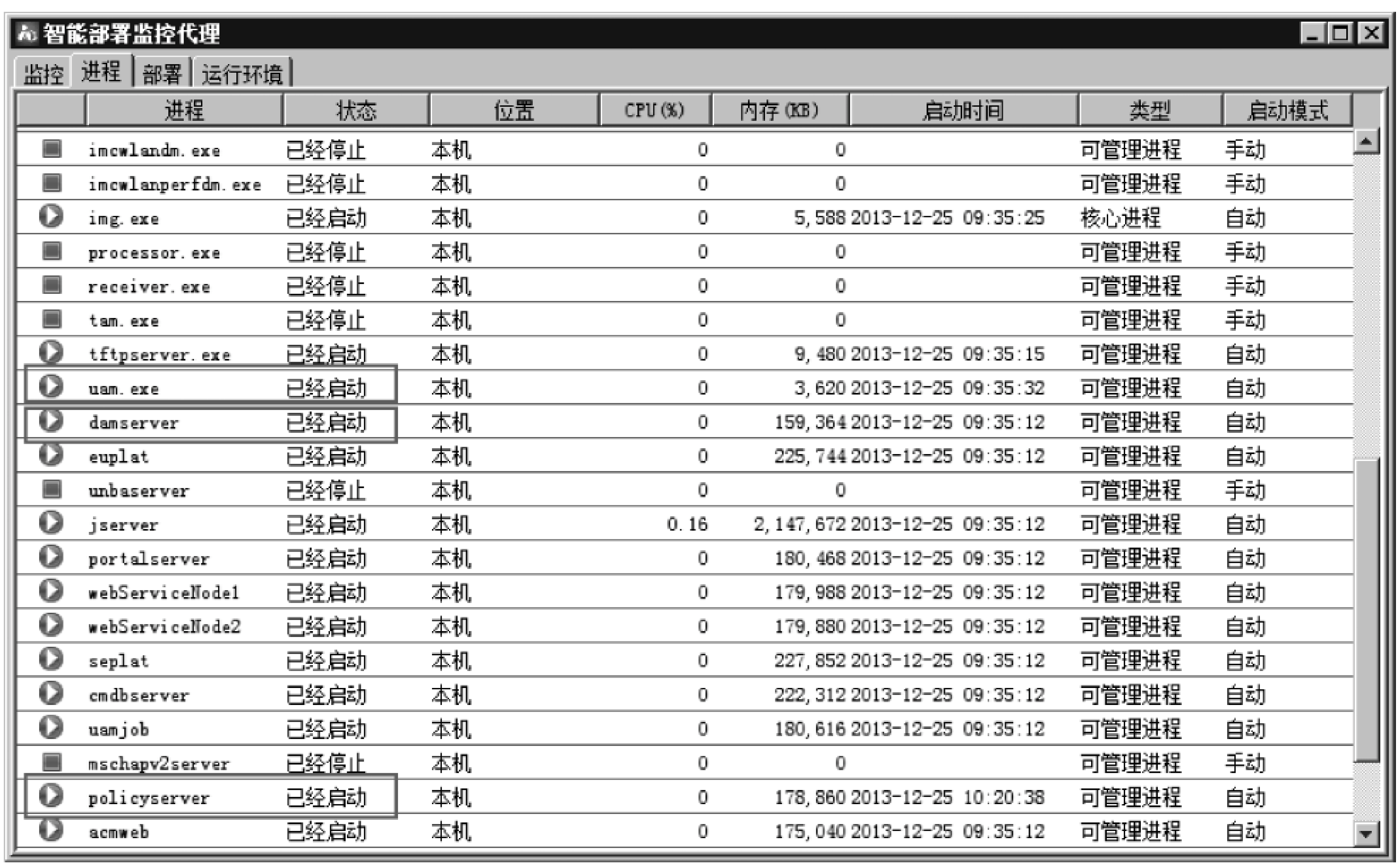


图 8-429　进程启动状态

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

② 检查服务器 9029 UDP 端口是否被 damserver 相关进程所监听，由于 damserver 是

java 进程，在任务管理器中找到对应进程为 java 即可，如图 8-430 所示。



图 8-430　任务管理器中的 java 进程

说明：

(a) Windows 操作系统中，通过

netstat -aon | findstr :端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

举例：对于命令提示符回显，如图 8-431 所示。



图 8-431　命令提示符

其中第一列 UDP 所指监听的协议；第二列 0.0.0.0:9029 所指监听的服务器的 IP 和端口号，0.0.0.0 代表监听所有 IP 地址；第三列 *:* 代表此行信息为监听状态；最后一列 19420 代表此协议监听的进程 PID。

(b) 查到端口所对应的进程 PID 后，请查看 Windows 任务管理器，9029 端口所对应的应为 damserver 为 java 进程。

(10) DAM 服务器和 DAM 客户端连通性检查

需检查在客户端认证上线后，服务器到客户端的可达性。在未禁止 ping 的环境中，可使用简单的 ping 进行测试。如 ping 不通，需先将网络调通。

(11) DAM 客户端在线状态检查

在 iMC 配置页面资产列表中，需要下发软件的 PC 状态需要为在线状态。如终端不符合，需按照云图《桌面资产管理故障排查》先进行排查。

(12) DAM 服务器配置检查

DAM 服务器的配置流程分为两大步：配置软件分发服务器和定制软件分发任务。

配置较为简单，给出 HTTP、FTP、文件服务器 3 种服务器的配置截图供排错参考。

① HTTP 分发服务器。

图 8-432 所示为 HTTP 分发服务器。

HTTP 分发任务如图 8-433 所示。



图 8-432 HTTP 分发服务器



图 8-433 HTTP 分发任务

对于静默安装和交互安装的安装类型，需要注意软件名称处配置。软件名称需要和下发的软件安装后在添加和删除程序中的名称完全一致，如图 8-433 中的软件，安装后在客户端“控制面板”→“所有控制面板”→“程序和功能”条目中，如图 8-434 所示。

② FTP 分发服务器。

图 8-435 所示为 FTP 分发服务器。

FTP 分发任务如图 8-436 所示。



图 8-434 "程序和功能"条目



图 8-435 FTP 分发服务器



图 8-436 FTP 分发任务

③ 文件服务器。

图 8-437 所示为文件服务器。



图 8-437 文件服务器

文件服务器分发任务如图 8-438 所示。

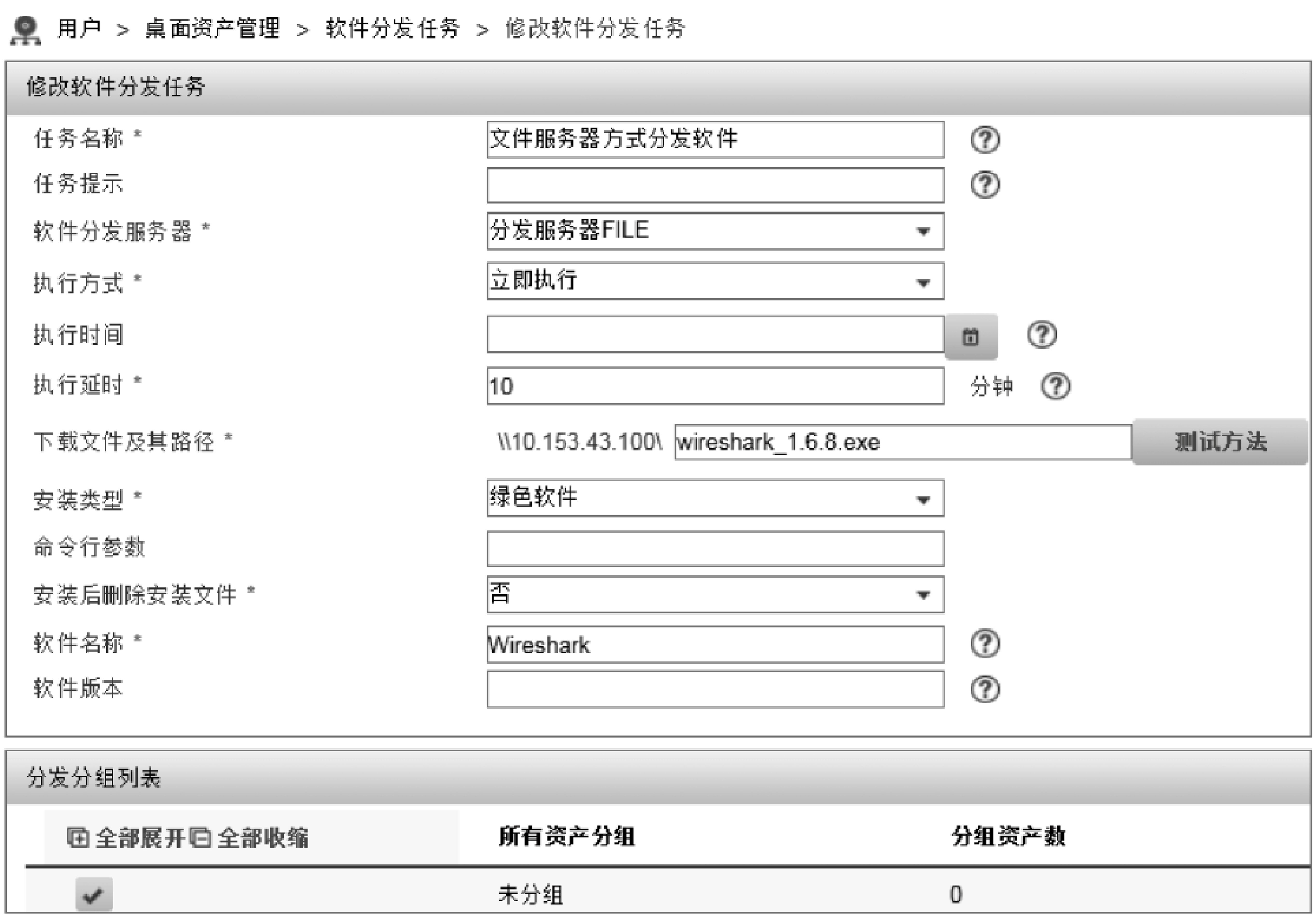
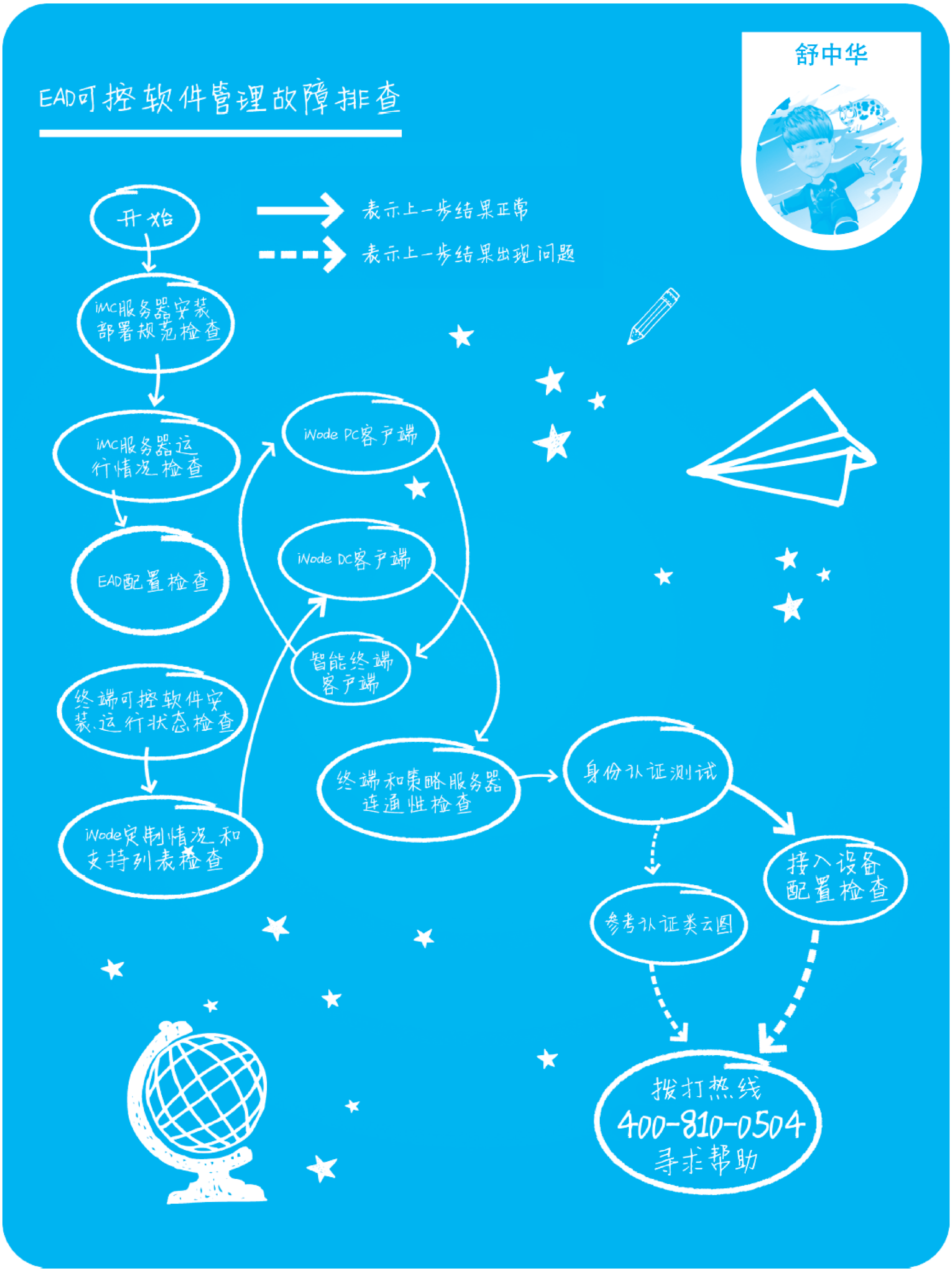


图 8-438 文件服务器分发任务


舒中华
EAD可控软件管理故障排查
开始
表示上一步结果正常
表示上一步结果出现问题
iMC服务器安装部署规范检查
iMC服务器运行情况检查
EAD配置检查
终端可控软件安装、运行状态检查
iNode定制情况和支持列表检查
iNode PC客户端
iNode DC客户端
智能终端客户端
终端和策略服务器连通性检查
身份认证测试
接入设备配置检查
参考认证类云图
拨打热线
400-810-0504
寻求帮助

1. 开始

EAD 可控软件管理即黑白软件管理，黑名单顾名思义不允许安装运行，白名单则允许安装运行。此外，还支持纯白软件管理，即要求终端必须安装软件列表里的应用程序，可以对软件、进程、服务、文件等进行匹配，并根据灵活的控制策略将不满足策略要求的终端进行隔离、下线、提醒等，保证必备软件的正常安装运行，将安全投资落到实处，巩固终端安全。

EAD 可控软件管理排错思路：身份认证之后才会触发安全认证，关于身份认证失败的排查思路可以参考具体的认证类云图，在此不再叙述。首先检查服务器软硬件及性能是否满足当前认证需要，然后从 iNode PC 和 iNode DC 及智能终端 3 种客户端认证场景进行分析，做相应 iMC 服务器运行状态的检查，安全策略配置检查，终端软件安装情况检查，最后对照 iNode 版本说明书查看支持的检查项及注意事项。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、Portal 网页在线数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“EAD 安全策略管理”各组件是否已部署的状态，具体如图 8-439 所示，关于“用户接入管理”组件的检查方式，请参考认证类云图。



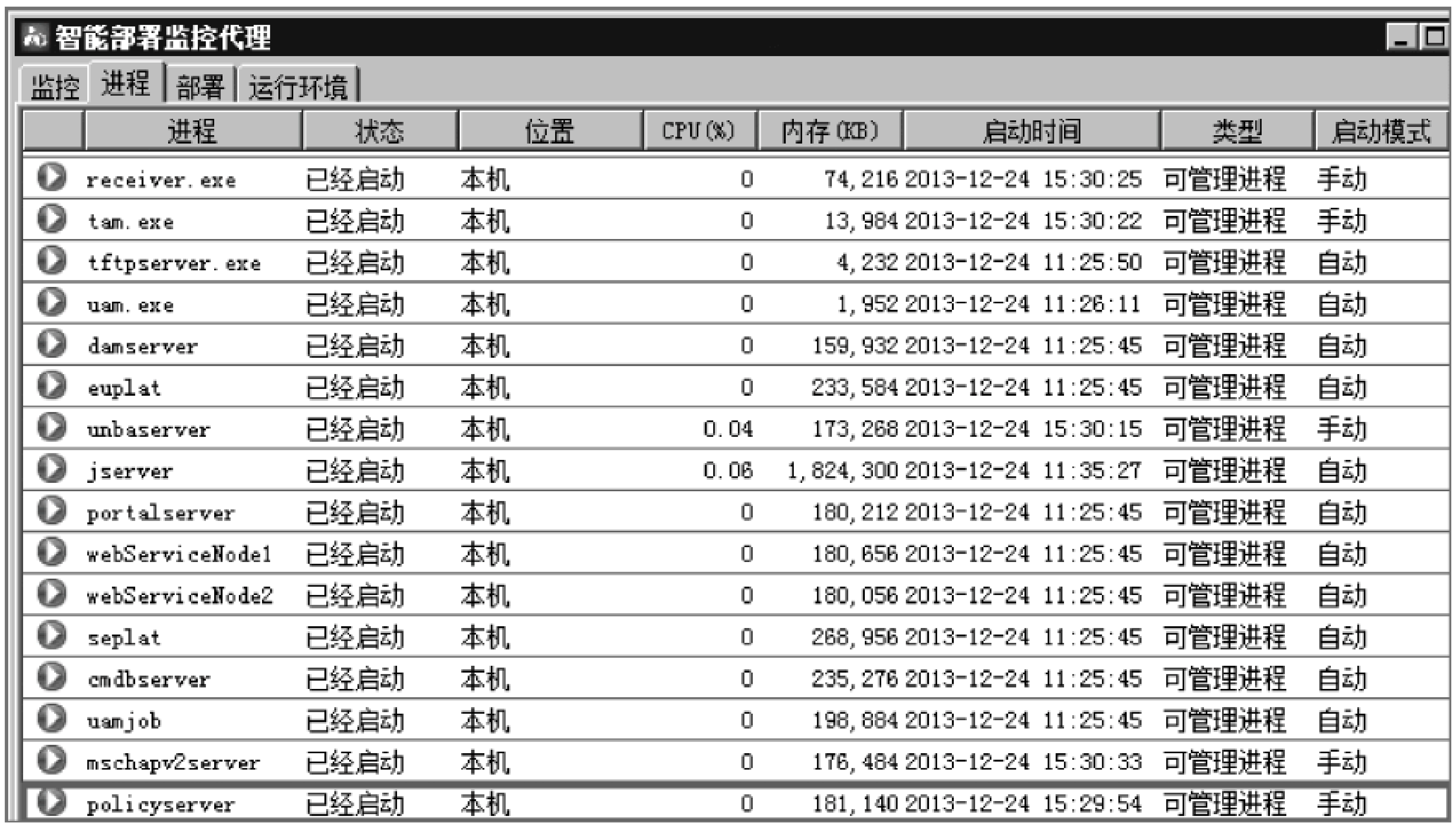
图 8-439 组件部署情况

说明： EAD 安全策略管理—桌面资产管理和 EAD 安全策略管理—桌面资产管理代理服务器是桌面资产(DAM)管理的功能组件，在 EAD 解决方案中可以不部署。

（2）iMC 服务器运行情况检查

要使用可控软件管理功能，除了确保 UAM 相关进程运行正常外，还要检查策略服务器对应的进程是否运行正常，及进程绑定的端口是否正常，具体可从如下两方面检查。

① 单击“开始”→“智能部署监控代理”命令，选择“进程”标签，查看 EAD 的核心进程 policyserver 是否正常启动，具体如图 8-440 所示。



进程	状态	位置	CPU(%)	内存(KB)	启动时间	类型	启动模式
receiver.exe	已经启动	本机	0	74,216	2013-12-24 15:30:25	可管理进程	手动
tam.exe	已经启动	本机	0	13,984	2013-12-24 15:30:22	可管理进程	手动
tftpserver.exe	已经启动	本机	0	4,232	2013-12-24 11:25:50	可管理进程	自动
uam.exe	已经启动	本机	0	1,952	2013-12-24 11:26:11	可管理进程	自动
dmserver	已经启动	本机	0	159,932	2013-12-24 11:25:45	可管理进程	自动
euplat	已经启动	本机	0	233,584	2013-12-24 11:25:45	可管理进程	自动
unbaserver	已经启动	本机	0.04	173,268	2013-12-24 15:30:15	可管理进程	手动
jserver	已经启动	本机	0.08	1,824,300	2013-12-24 11:35:27	可管理进程	自动
portalserver	已经启动	本机	0	180,212	2013-12-24 11:25:45	可管理进程	自动
webServiceNode1	已经启动	本机	0	180,656	2013-12-24 11:25:45	可管理进程	自动
webServiceNode2	已经启动	本机	0	180,056	2013-12-24 11:25:45	可管理进程	自动
seplat	已经启动	本机	0	268,956	2013-12-24 11:25:45	可管理进程	自动
cmdbserver	已经启动	本机	0	235,276	2013-12-24 11:25:45	可管理进程	自动
uamjob	已经启动	本机	0	198,884	2013-12-24 11:25:45	可管理进程	自动
mschapv2server	已经启动	本机	0	176,484	2013-12-24 15:30:33	可管理进程	手动
policyserver	已经启动	本机	0	181,140	2013-12-24 15:29:54	可管理进程	手动

图 8-440　进程正常启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

② 检查策略服务器对应的监听端口 UDP 9019，UDP 9017 是否正常绑定，如图 8-441 所示。

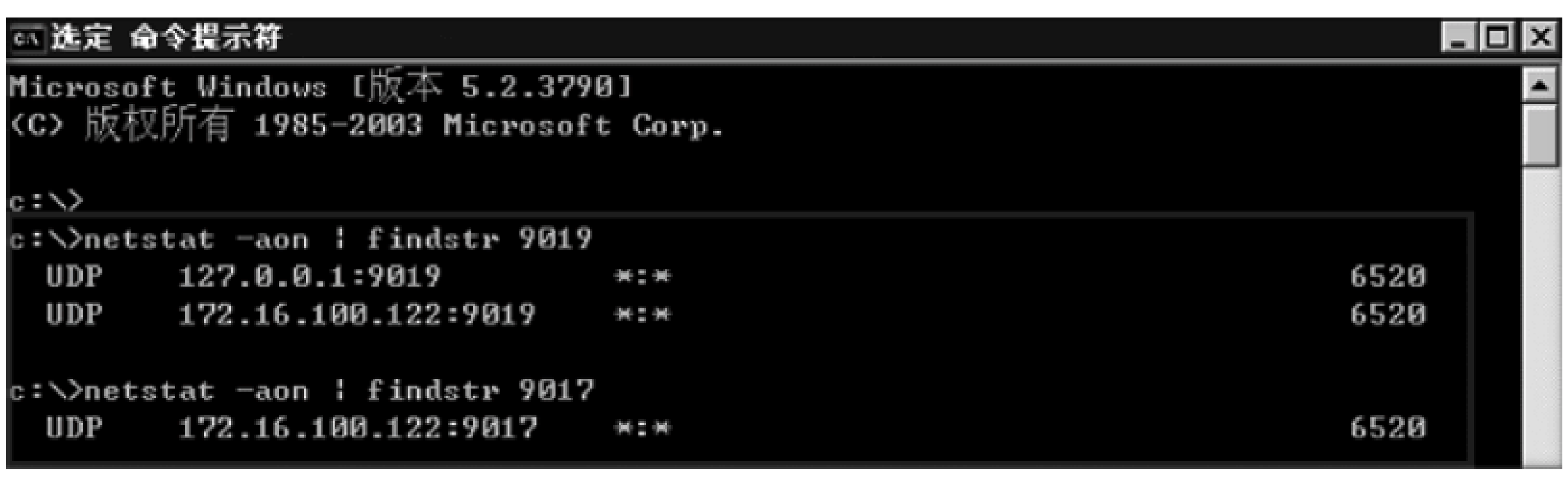


图 8-441　端口正常绑定情况

说明 1：如图 8-441 所示，9019 端口号必须同时绑定两个 IP，分别是 127.0.0.1 和实际网卡 IP：172.16.100.122，而 9017 端口只需绑定实际网卡 IP 即可，如图 8-442 所示。

说明 2：Windows 操作系统中，通过命令 netstat -aon |findstr 端口号来显示某端口的监听状态以及对应的进程 PID，举例：对应提示符回显，如图 8-443 所示。

其中第一列 UDP 监听的协议；第二列 172.16.100.122：9017 所指监听的服务器的 IP 和端口号；第三列 *.* 代表监听状态；最后一列 6520 代表此协议监听的进程 PID，根据此 PID，对照 Windows 任务管理器，即可确定该端口绑定的具体服务。

（3）EAD 配置检查

① 可控软件策略配置检查。要实施可控软件管理，首先必须配置可控软件组，例如：要控制终端不能运行 QQ 软件，则必须先创建一个包含可控软件组，并绑定一个检查项，可根据进程、服务、文件或软件创建该检查项。举例：如图 8-444 所示。



图 8-442　绑定两个 IP



图 8-443　提示符回显



图 8-444　配置可控软件组

说明 1：在增加进程时，可以单击对应Ⓘ的来获取帮助信息，如图 8-445 所示。



图 8-445　获取帮助信息

说明 2：

(a) 可控软件组的类型包括进程、服务、文件及软件。不同的类型配置可能不同，在 EAD 安全策略中的检查类型也有区别，例如：如图 8-446 所示，当“类型”为“软件”时，其检查类型包含“禁止安装”“必须安装”“仅限安装”，如图 8-447 所示。

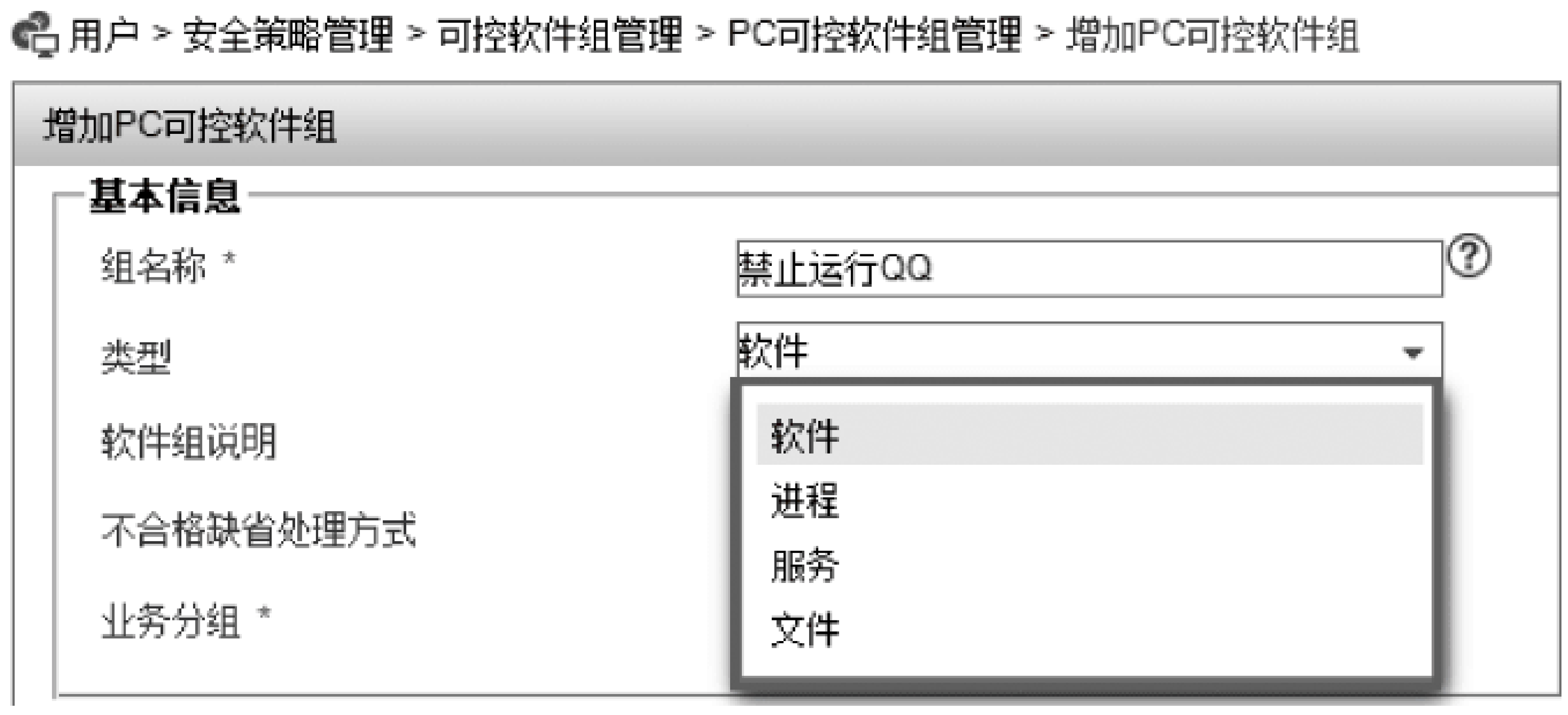


图 8-446　类型选为软件



图 8-447　检查类型

而当“类型”为“进程”时，其检查类型只包含“禁止运行”和“必须运行”。“类型”为“服务”时，其检查类型包含“禁止启动”和“必须启动”，“类型”为“文件”时，其检查类型为“必须存在”和“禁止存在”，如图 8-448 所示。



图 8-448　类型与检查类型

(b) 一个可控软件组可以包含多个检查项。可控软件组中的软件/进程/服务/文件之间是“或”关系，即只要一个条件满足，就采取相应的措施。分以下两种情况来说明。

ⓐ PC 可控软件组“A”中，定义了诺顿、金山毒霸和瑞星 3 个软件。在安全策略中要求客户端必须安装 PC 可控软件组“A”中的软件，则此时客户端只要安装了诺顿、金山毒霸或瑞星其中之一，安全检查即通过；否则安全检查不通过。

ⓑ PC 可控软件组“B”中，定义了 QQ、MSN 两个软件。在安全策略中要求客户端禁止安装 PC 可控软件组“B”中的软件，则此时客户端只要安装了 QQ、MSN 其中之一，安全检查不通过；只有客户端既没有安装 QQ 也没有安装 MSN 时，安全检查才能通过。

然后创建安全策略，并将创建的可控软件组和安全级别绑定。然后在“服务”里绑定“安全策略”，如图 8-449 所示。



图 8-449 在"服务"里绑定"安全策略"

说明：安全级别可自行定义，默认包含监控、VIP、隔离、下线、访客 5 个级别，不同安全级别的控制策略有所不同，具体如下。

(a) 监控模式：无论安全检查结果如何，都提示用户通过安全检查，不弹出安全检查结果页面，不对用户做任何限制。只在服务器一侧记录检查结果以备之后审计。

(b) VIP 模式：若安全检查不通过则会提示用户存在安全隐患，但不对用户采取任何动作，不弹出安全检查结果页面。

(c) 隔离模式：若安全检查不通过，通知安全联动设备限制用户只能访问隔离区资源。

(d) 下线模式：若安全检查不通过，将用户强制下线。

(e) 访客模式：特殊的下线模式，默认设置了"不安全提示阈值"。

最终，接入账号和服务进行绑定，总之，只有账号绑定了正确的"服务"，"服务"绑定了正确的"安全策略"，"安全策略"绑定了正确的"安全级别"和"可控软件策略"，才会进行可控软件的检查。检查账号是否配置了正确的可控软件策略最直观的方法：通过接入账号确定其绑定的服务，然后通过服务确定其绑定的安全策略，通过安全策略可以检查具体的可控软件策略和安全级别，包括安全级别及下发的 ACL、VLAN 配置是否正确等，如图 8-450 所示。

② 授权配置检查。

当终端不满足可控软件策略时，会将该用户下线或放到隔离区，而隔离区的构造通常通过下发 ACL 或 VLAN 实现，在使用 ACL 或 VLAN 进行授权场景，需要确保下发后终端 PC 和策略服务器能正常通信，如图 8-451 所示。

例如：终端 PC 的 IP：192.168.100.1，策略服务器 IP：172.16.100.200，如果使用 ACL 进行授权，则设备侧的 ACL 配置中必须有放通源 IP:192.168.100.1，目的 IP:172.16.100.200 的 rule，如图 8-452 所示。

如果 ACL 是下发给 iNode 客户端，服务器侧的客户端 ACL 配置中也必须有放通目的 IP 为策略服务器 172.16.100.200 的规则，如图 8-453 所示。

说明：EAD 构造隔离区有下发 ACL 和 VLAN 两种，而 ACL 可以下发给设备，也可以下发给 iNode 客户端，VLAN 只能下发给设备，向接入设备下发接入用户所使用的 VLAN，可以下发 VLAN ID，也可以下发 VLAN NAME，如果下发 VLAN ID，则 VLAN ID 必须在 1～

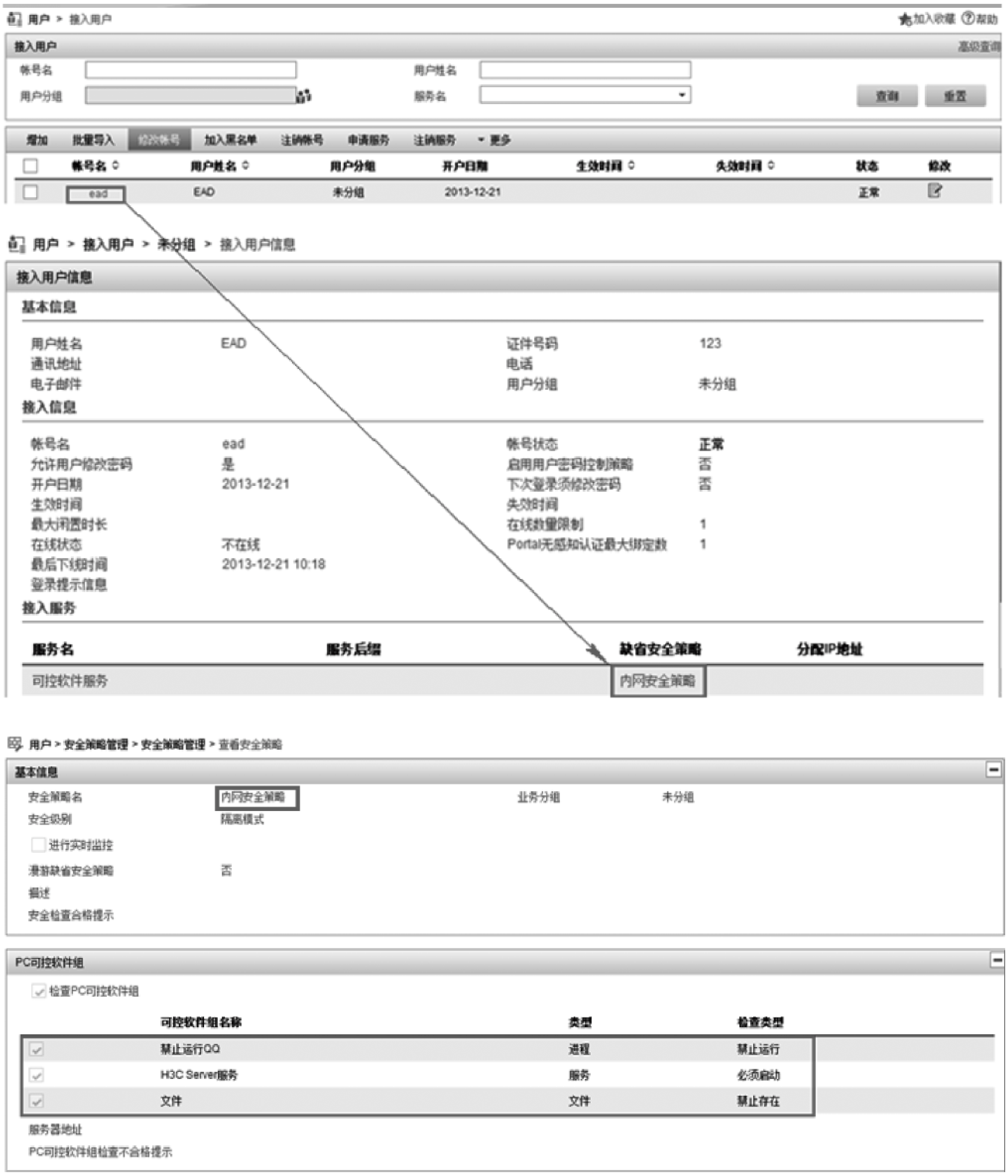


图 8-450　账号和服务绑定



图 8-451　向设备下发 ACL

```
acl number 3000
 rule 0 permit ip source 192.168.100.1 0 destination 172.16.100.200 0
 rule 1 deny ip
```

图 8-452　终端 PC



图 8-453　服务器侧的客户端 ACL 配置

4094 之间，如果接入设备上不存在此 VLAN ID，则会自动创建，如果下发 VLAN NAME，接入设备上必须预先创建此 VLAN NAME，否则下发的 VLAN 无效。如果 ACL 下发给设备，则必须预先在设备侧配置好 ACL，如果 ACL 下发给 iNode 客户端，则 ACL 规则需要在 iMC 服务器侧配置，并且 iNode 需要定制客户端 ACL 功能，如图 8-454 所示。

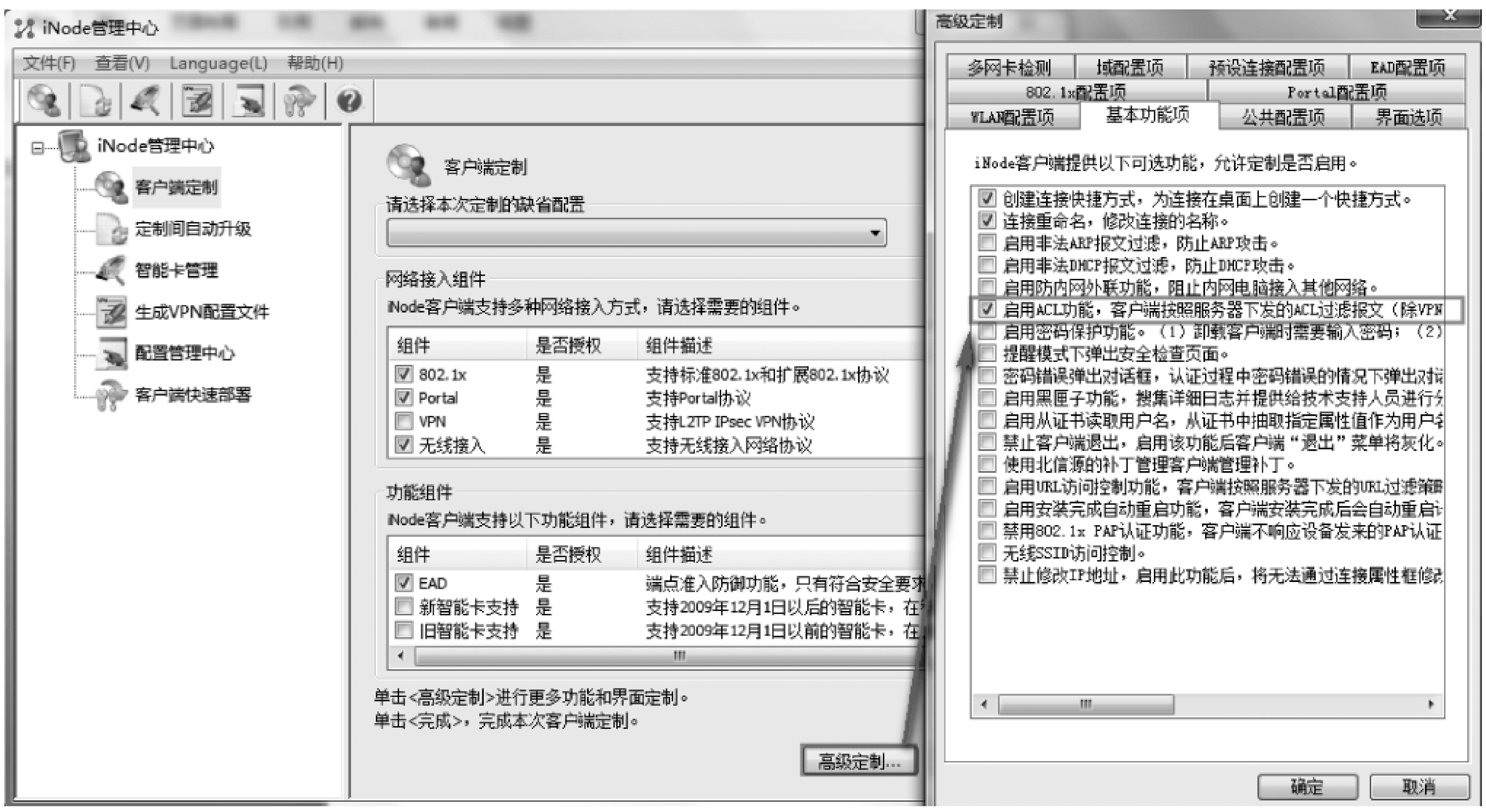


图 8-454　高级定制

（4）终端可控软件安装、运行状态检查

EAD 可控软件管理可以检测终端 PC，包括 Windows、Linux、Mac OS 操作系统以及智能终端 Android 系统是否满足可控软件策略要求。在实施或定位可控软件管理相关问题时，如果通过以上步骤排查都未发现异常，接下来就需根据服务器侧的可控软件策略排查终端软件安装、运行情况。以 Windows 和 Android 系统为例，从进程、服务、软件、文件说明排查方法。

① 查看 Windows 系统的进程运行状态。

对于 Windows 操作系统，进程名称必须与“任务管理器”→“进程”中软件的映像名称保持一致，如图 8-455 所示。对于 Linux 操作系统，进程名称必须与 ps -ef 命令结果中的进程名称保持一致；对于 Mac OS，进程名称必须与 ps -awwx -o command 命令果中的进程名称保持一致。进程名称不允许包含{、|、<、>、/、%、&、'、\、"、,、;、*、}等特殊字符。

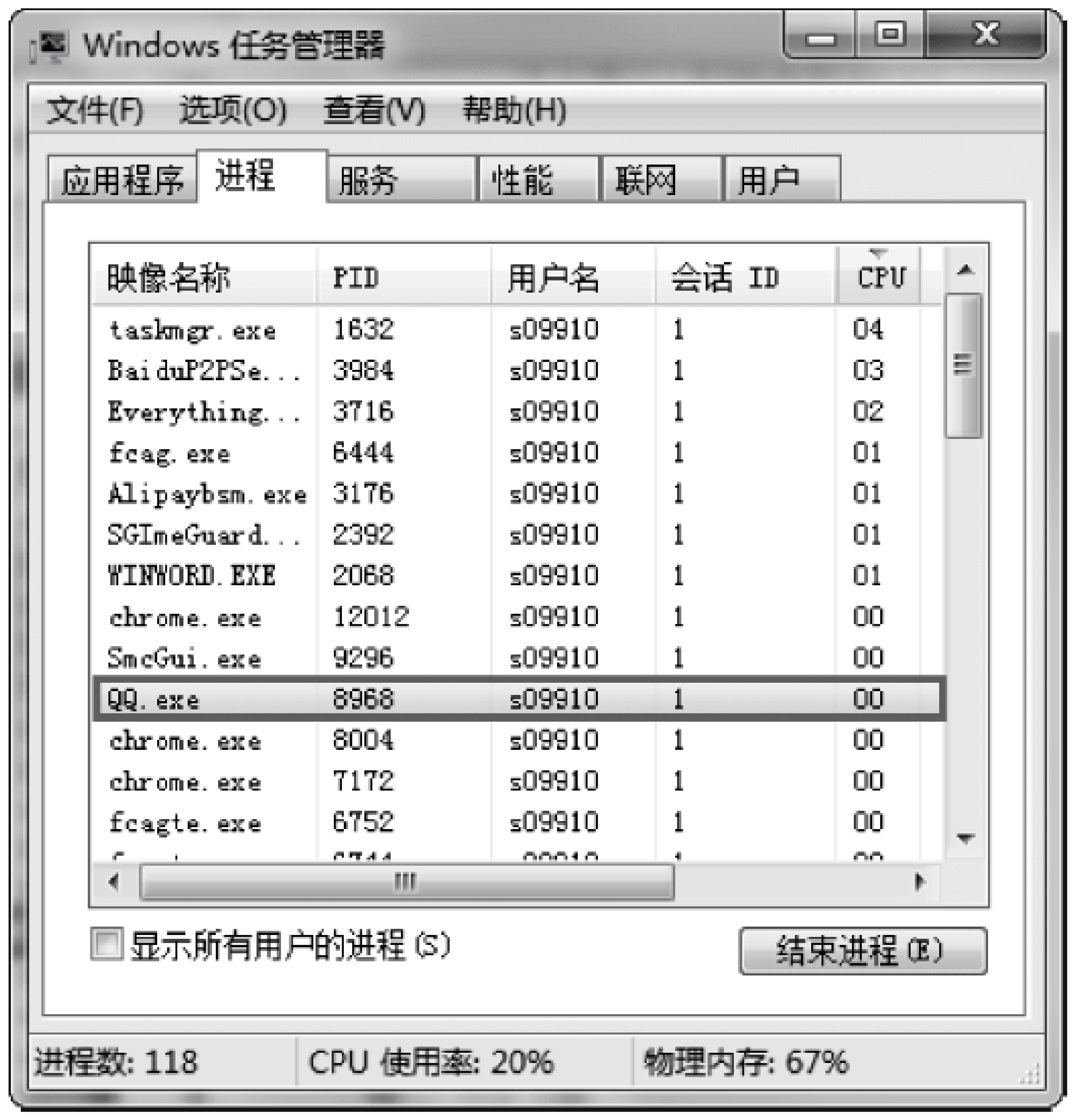


图 8-455　软件映像名称保持一致

说明：

(a) iNode 客户端不检查带有“/”的系统内核进程。例如：iMC 要求检查 events 进程，则 iNode 客户端不会检查类似 events/0 的系统内核进程，而只检查类似 warning/events 的非系统内核进程。

(b) 在 PC 可控软件组中增加进程时，还可以设置检查类型，而软件和服务不能设置检查类型。检查类型为简单检查指客户端不检查伪进程；检查类型为复杂检查指客户端要检查伪进程(注：伪进程是指进程的实际名称与在“任务管理器”→“进程”中软件的进程名不一致的进程)。MD5 检查是一种更高级的检查方式。管理员计算软件的 MD5 摘要(推荐使用 iMC 自带的计算工具计算 MD5 摘要)，工具下载路径，如图 8-456 所示。



图 8-456　工具下载路径

根据可执行文件计算出 MD5 摘要，如图 8-457 所示。

在可控软件组中配置，如图 8-458 所示。

通过 iMC 将摘要下发给 iNode 客户端，iNode 客户端根据服务器下发的 MD5 摘要检查终端用户是否运行了摘要对应的软件。对必须运行的某个进程执行 MD5 检查的规则：在 Windows 任务管理器中匹配该进程对应的进程名称，匹配 iMC 中配置的该进程对应的 MD5 码。如果两者都匹配，安全检查合格；否则安全检查不合格。对禁止运行的某个进程执行 MD5 检查的规则：在 Windows 任务管理器中匹配该进程对应的进程名称，匹配 iMC 中配置



图 8-457　计算 MD5 摘要



图 8-458　在可控软件中配置

的该进程对应的 MD5 码。只要两者有一个匹配，安全检查就不合格；反之安全检查合格。

进程的复杂检查和 MD5 检查方式只适用于 Windows 操作系统，Linux 和 Mac OS 不支持。

② 查看 Windows 系统服务启动状态。

对于 Windows 操作系统，iMC 服务器侧可控软件组配置里的“服务名称”必须与单击“控制面板”→“管理工具”→“服务”→“属性”命令后的服务名称保持一致，如图 8-459 所示。对于 Linux 操作系统，服务名称必须与 service-status-all 命令结果中的服务名称保持一致；对于 Mac OS，服务名称必须与 service-list 命令结果中的服务名称保持一致。服务名称不允许包含{、|、<、>、/、%、&、'、\、"、,、;、* 、}等特殊字符。



图 8-459　“服务名称”与“属性”服务名称一致

iMC 服务器侧相应配置如图 8-460 所示。



图 8-460　iMC 服务器侧相应配置

③ 查看 Windows 系统软件的安装状态。

PC 可控软件组中的软件名称必须与单击"控制面板"→"添加或删除程序"命令后软件的名称保持一致。软件名称不允许包含{、;、*、}等特殊字符，如图 8-461 所示。



图 8-461　Windows 系统软件的安装状态

④ 查看 Windows 系统文件的存在状态。

PC 可控软件组中配置文件时，文件路径和名称就是文件的绝对路径+文件名。文件名需包含扩展名，且不允许包含{、*、?、;、|、#、<、>、}，如图 8-462 所示。

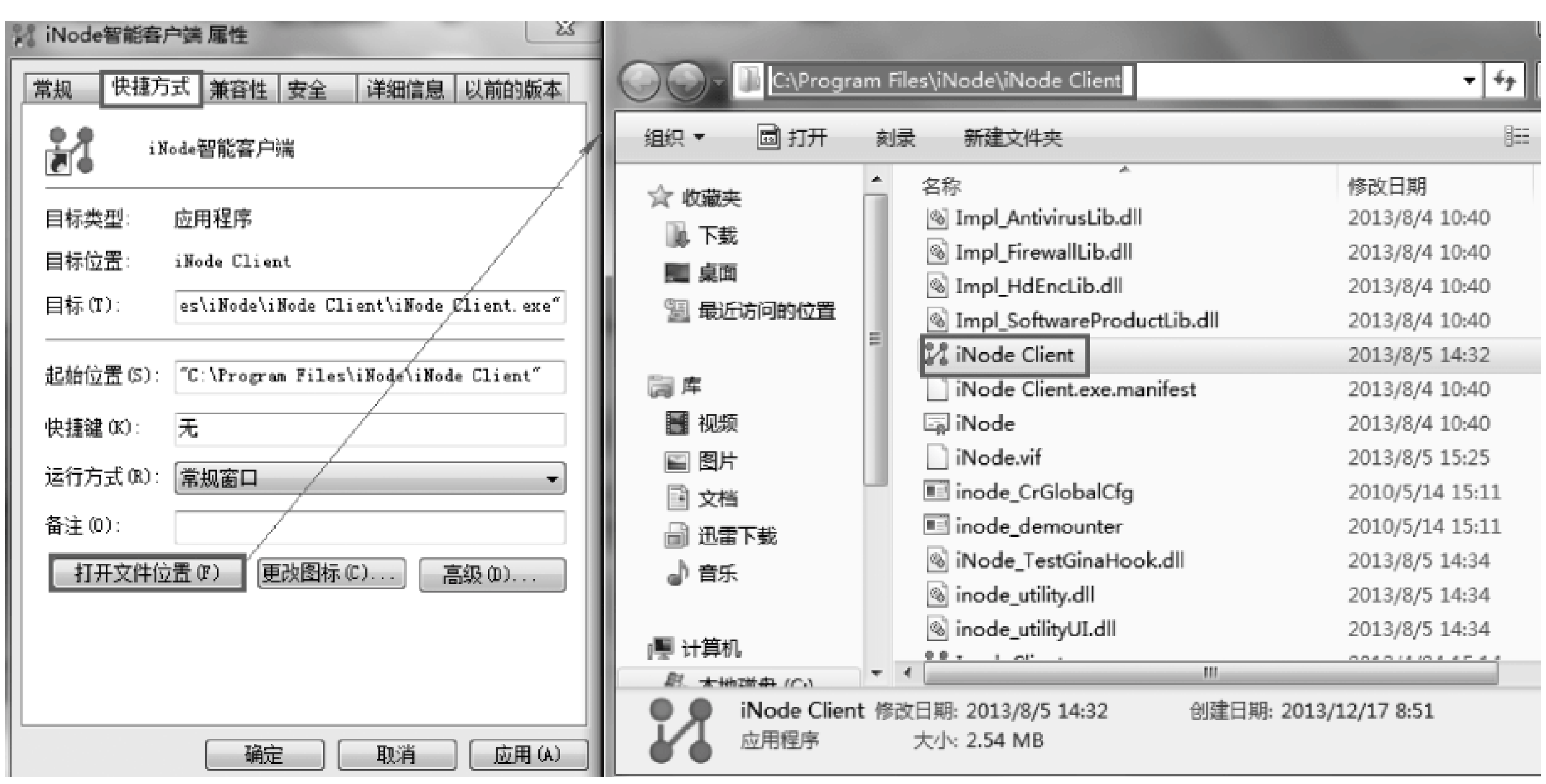


图 8-462　文件名

iMC 服务器侧相应配置如图 8-463 所示。



图 8-463　iMC 服务器侧相应配置

⑤ 查看 Android 系统软件的安装状态。

智能终端可控软件管理当前只支持 Android 系统的软件安装管理。

并且智能终端可控软件组中的软件名称必须与单击系统的“设置”→“应用程序”→“管理应用程序”命令后软件的名称保持一致。软件名称不允许包含{、;、*、}等特殊字符，如图 8-464 所示。



图 8-464　软件名称规定

iMC 服务器侧相应配置如图 8-465 所示。



图 8-465　相应配置

说明：Andriod 系统新版本查看软件名称的路径为：“设置”→“应用程序”。

(5) iNode 定制功能和支持列表检查

H3C iNode 包含 iNode PC(包含 Windows、Linux、Mac OS)、iNode DC、iNode MC 3 种。

针对 Windows 系统的 iNode PC 客户端需要先安装 iNode 管理中心，然后根据需要定制 iNode 安装/升级包，EAD 可控软件管理功能必须依赖 iNode 客户端，并且必须定制 EAD 功能，查看方法及注意事项如下。

① 查看 iNode PC 是否定制了 EAD 功能：单击 iNode 菜单“信息”→“主机和网络相关信息”命令后打开如图 8-466 所示对话框，查看“客户端信息”标签，是否支持 EAD。

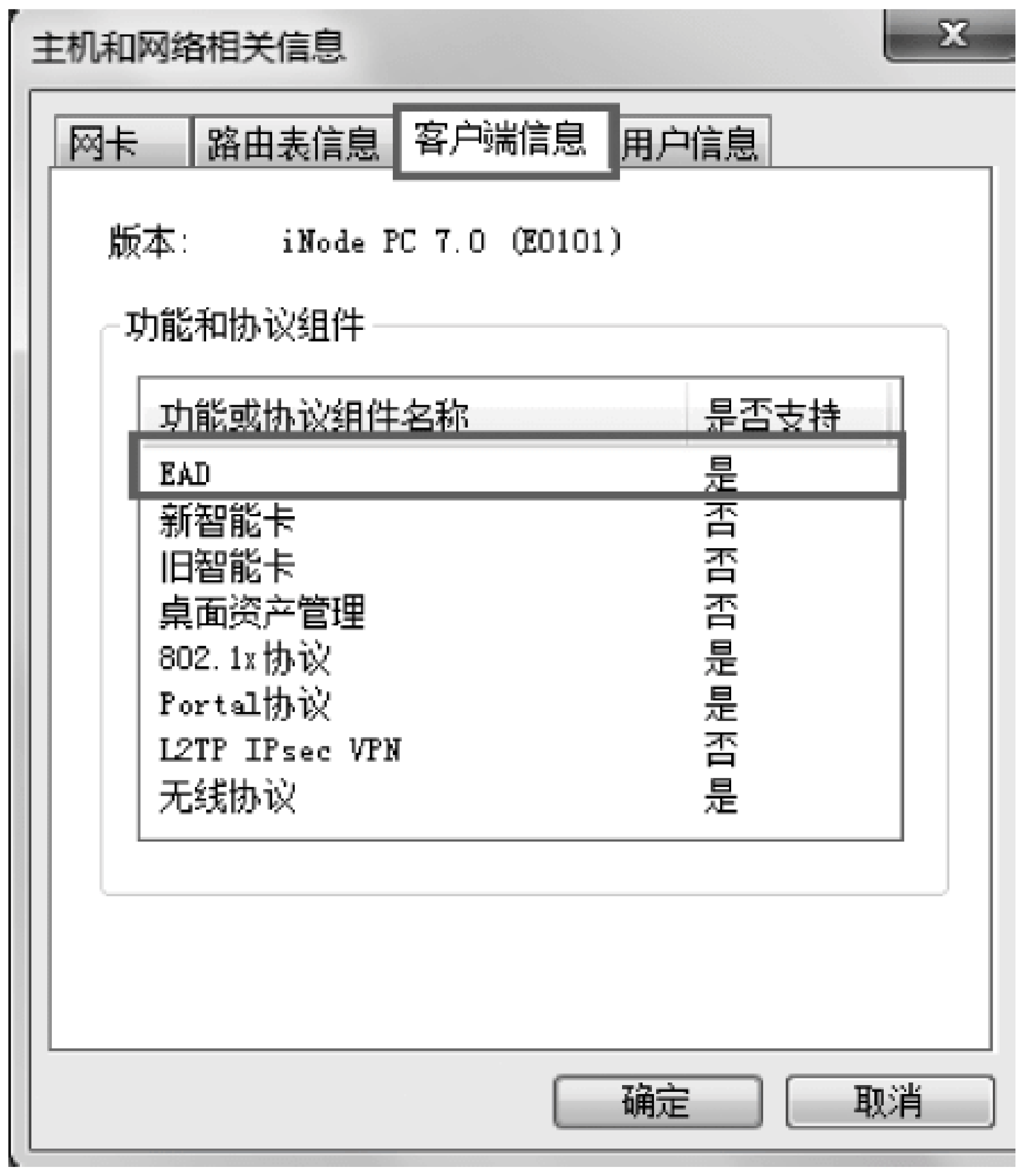


图 8-466 “客户端信息”标签

② iNode DC 即可溶解客户端，是 iNode PC 的一个子集，在 Portal 认证场景，如果未安装 iNode PC，但是要使用可控软件管理功能，则需要安装部署可溶解客户端，iNode DC 必须先在 iMC 服务器侧安装部署成功后才能使用，如图 8-467 所示。



图 8-467 iNode DC 必须在 iMC 服务器侧安装部署成功

③ 针对 Linux、MAC OS 以及 Android 系统的 iNode 安装包默认具有 EAD 功能。

当前 IOS 系统的 iNode 还不支持 EAD，故也不支持可控软件管理。

④ 查看 iNode 版本说明书，重点阅读版本使用限制和软件特性章节，如图 8-468 所示。

(6) PC 和策略服务器连通性检查

在开启策略服务器场景，即使没有开启可控软件管理功能，也需要确保终端 PC 和策略服务器能正常双向通信，否则，身份认证成功后会下线，其采用 UDP 协议进行通讯，策略服务器使用固定(默认为 9019)端口监听客户端消息，iNode 客户端也从固定监听端口(从 10102 开始递增的第一个空闲端口)发送和接受报文。如果中间有防火墙，需要放通 UDP 协议报文。对

软件，进程，服务，文件管理	• 支持黑白软件检查（仅支持 Windows 操作系统） • 支持黑白软件运行状态 MD5 检查（仅支持 Windows 操作系统） • 支持终端运行进程检查 • 支持终端运行服务检查 • 支持纯白软件（仅支持操作 Windows 系统） • 支持终端 PC 文件检查

图 8-468 iNode 版本说明书

于没有禁 ping 的环境，从 iMC 服务器上 ping 终端 PC 的 IP；对于禁 ping 的环境，有两种方法确定 PC 和策略服务器的连通性。

① 可以在策略服务器和终端 PC 侧同时抓包确定是否能正常通信，如图 8-469 所示。

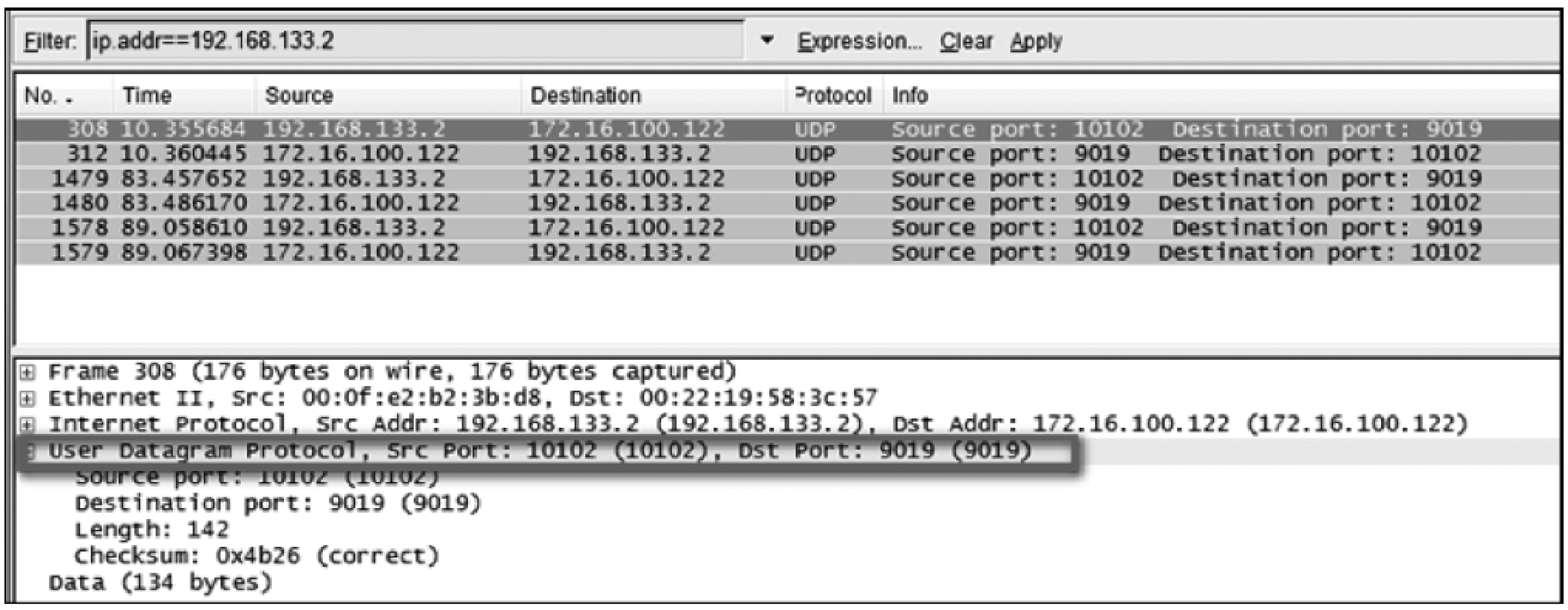


图 8-469 正常通信

说明：如图 8-469 所示，192.168.133.2 为终端 PC 的 IP，172.16.100.122 为策略服务器的 IP，在服务器和 PC 侧同时抓包可以看到其 UDP 报文的详细交互过程。

② 通过 iNode 和策略服务器的日志确定。

iNode 的 Detail 日志文件 secpkt.txt 如下。

```
[2012-02-10 10:42:26] [DtlCmn] [674] secPushInner: out-pkt [1]        //安全认证请求报文
<i n="userName">szh1@iMC</i>
<in="hwAddr">18:A9:05:DF:D4:0E</i>
<i n="eventSeqID">JOvPBgcC</i>
[2012-02-10 10:42:27] [DtlCmn] [1ba0] sndSecMsg: transfer [2] [11260]   //安全认证回应报文
<i n="heartBeatInterval">720</i>
<i n="heartBeatOutTimes">3</i>
```

策略服务器调试日志如下。

```
2012-02-10 08:57:38 [策略服务器] [信息(0)] [24] [ProxyRequestHandler::run] szh1@iMC ; EAD
认证上线请求报文(1) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2...文解析成功
                                                                //认证上线请求报文
2012-02-10 08:57:38 [策略服务器] [信息(0)] [15] [RequestProcessor::processRequest] szh1@iMC
; EAD 认证上线回应报文(2) ; kNIXeLUQ ;18:A9:05:DF:D4:0E ;  192.168.133.2 ;...
                                                                //认证上线回应报文
```

说明：如上的 iNode 日志级别需要设置为 Detail 才能看到具体的交互报文（日志存放路径：C:\Program Files\H3C\iNode Client\CollectInfo\＊），同理，策略服务器日志级别也需要

设置调试才能看到和 iNode 的详细报文交互(日志存放路径：iMC 安装目录\ead\logs\policyserver_ ****-**-**)；关于日志级别的设置方法请参考其他文档。

(7) 身份认证测试

身份认证成功后才会发起安全认证，在 EAD 安全认证前，必须确保能身份认证成功，如图 8-470 所示。



图 8-470　身份认证测试

说明：如果身份认证失败，请参考身份认证相关云图。

(8) 接入设备配置排查

如果身份认证成功后，却一直未触发安全认证，这里需分两种情况讨论。

① 如果接入设备是 H3C 类型，在 Portal+EAD 场景，则设备侧的 Radius Scheme 方案里的 Server-type 配置 Extended|Standard 都可以。在 Dot1x+EAD 场景，则 Radius Scheme 方案里的 Server-type 可以配置 Standard，但是 Dot1x Authencation-method 必须配置为 EAP 才能触发 EAD 认证，但是无法给设备下发 ACL 和 VLAN 进行授权，如果 ACL 下发给 iNode 不受影响，故，接入设备是 H3C 类型，在 EAD 开局中，建议将 Radius Scheme 的 Server-type 配置为 Extended。

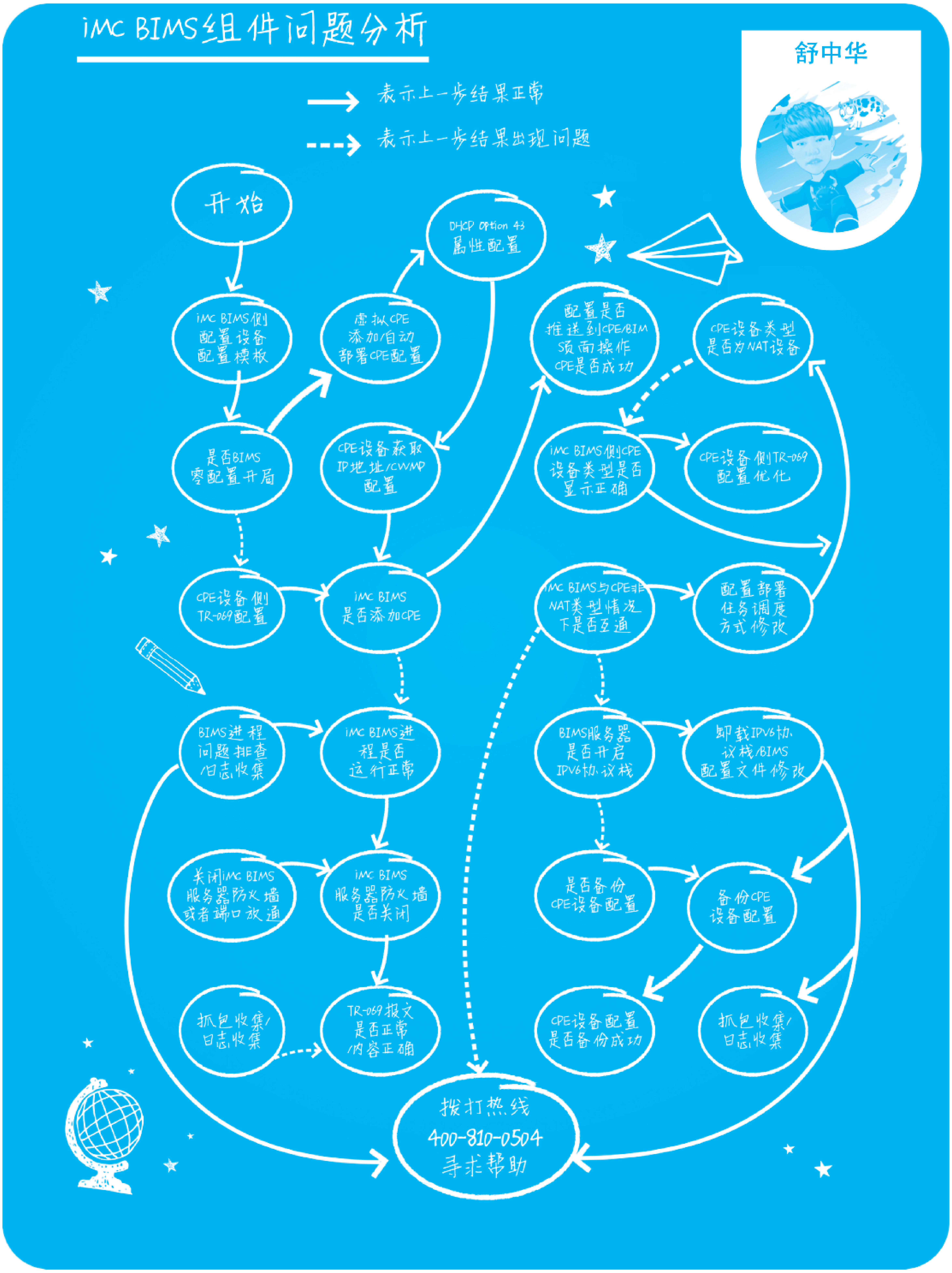
② 如果接入设备是第三方厂商，由于不支持 Portal 认证，在 802.1x 认证场景 Authentication-method 必须配置为 EAP 方式，否则不会触发安全认证。H3C 设备配置方法如图 8-471 所示。

```
radius scheme test
 server-type extended
```

```
[ywrj-121-C0re]dot1x authentication-method eap
 EAP authentication is enabled
```

图 8-471　H3C 设备配置

说明：结合第三方设备实施 EAD 解决方案，Dot1x+EAD 场景，Dot1x authentication-method 必须配置为 EAP，如果是 L2TP VPN+EAD，则接入设备必须为 H3C 设备，因为第三方设备的 Radius Scheme 不支持 Extended，且 VPN 认证方式不支持 EAP，故不支持 EAD。



iMC BIMS组件问题分析
舒中华
表示上一步结果正常
表示上一步结果出现问题
开始
iMC BIMS侧配置设备配置模板
是否BIMS零配置开局
CPE设备侧TR-069配置
虚拟CPE添加/自动部署CPE配置
DHCP Option 43属性配置
CPE设备获取IP地址/CWMP配置
iMC BIMS是否添加CPE
BIMS进程问题排查/日志收集
iMC BIMS进程是否运行正常
关闭iMC BIMS服务器防火墙或者端口放通
iMC BIMS服务器防火墙是否关闭
抓包收集/日志收集
TR-069报文是否正常/内容正确
配置是否推送到CPE/BIMS页面操作CPE是否成功
CPE设备类型是否为NAT设备
iMC BIMS侧CPE设备类型是否显示正确
CPE设备侧TR-069配置优化
iMC BIMS与CPE非NAT类型情况下是否互通
配置部署任务调度方式修改
BIMS服务器是否开启IPv6协议栈
卸载IPv6协议栈/BIMS配置文件修改
是否备份CPE设备配置
备份CPE设备配置
CPE设备配置是否备份成功
抓包收集/日志收集
拨打热线
400-810-0504
寻求帮助

1. 开始

分支网点管理(Branch Intelligent Management System，BIMS)通过 TR-069 协议对 CPE 进行远程集中管理，能够解决 CPE 量大、动态 IP 等管理困难，节约维护成本，提高问题解决效率，以满足对 CPE 在运营商解决方案中的管理需求。

日常局点对 iMC BIMS 组件的使用主要有部署、CPE 设备添加、CPE 配置推送以及 CPE 配置的备份等过程细节。本流程也将以上述 BIMS 的使用过程细节为主线，将开局以及运维中可能遇到的问题做一详细说明。

说明：iMC 服务器在网顺利运行的前提之一便是 iMC 服务器的安装部署符合相关规范。在 iMC BIMS 使用前请先判断 iMC 服务器的物理性能是否足够承载相关业务，重要组件是否分布式部署。相关部署要求规范请参考《智能管理中心(iMC)部署和硬件配置方案》。

2. 流程图相关操作说明

(1) iMC BIMS 侧配置设备配置模板

局点使用 iMC BIMS 组件的目的之一便是用其来向数量巨大的局端 CPE 设备推送相关配置，且不论是否为 BIMS 零配置开局要实现该功能的前提便是在 BIMS 侧配置好相关配置模板。登录 iMC 首页，依次单击“业务”→“分支网点管理”→“配置管理”→“配置模板库”→“增加配置模板”命令便可创建一 CPE 配置模板。本例中，配置模板的内容为修改 CPE 设备的设备名称，配置模板名称为“device_name_modify.cfg”，具体配置如图 8-472 所示。



图 8-472　模板配置

相关参数配置好之后，单击“确定”按钮，便可在单击“业务”→“分支网点管理”→“配置管理”→“配置模板库”命令后的目录下看到该新建的配置模板库及其对应的描述信息，如

图 8-473 所示。



图 8-473 新建模板库及描述信息

（2）是否为 BIMS 零配置开局

是否为 BIMS 零配置开局主要指的是设备在加电启动之后，配置内容中已经包含了 TR-069 协议相关配置，且其他设备运行配置由 BIMS 再次推送。TR-069 配置可配置的方式有 CLI 命令行配置、U 盘启动配置、DHCP Option 43 属性下发配置以及配置短信推送。具体选择何种方式来实现 BIMS 零配置，需要参考局点现场的网络环境。由于篇幅所限，本例中后续将以 DHCP Option 43 属性为例说明。

（3）虚拟 CPE 添加/自动部署 CPE 配置

在实现 BIMS 零配置的场景下，需要在 BIMS 上创建一虚拟 CPE 以及一针对该虚拟 CPE 的自动部署任务。该虚拟 CPE 包含了将来要添加的实体 CPE 的 OUI 以设备序列号信息，当实际 CPE 加入到 BIMS 时，系统会自动调用先前创建的配置部署任务，将相关配置推送到实际 CPE。

登录 iMC 首页，依次单击“业务”→“分支网点管理”→“增加 CPE”命令，如图 8-474 所示。



图 8-474 “增加 CPE”

相关 CPE OUI 以及序列号可以通过在 CPE 设备执行如下命令获取。

```
[CPE]display device manuinfo
Slot 2:
```

```
DEVICE_NAME              : S5800-56C
DEVICE_SERIAL_NUMBER     : 210235A377H11A000105
MAC_ADDRESS              : C4CA-D9B9-AF38
MANUFACTURING_DATE       : 2012-05-24
VENDOR_NAME              : H3C
```

或者也可以查看设备机框上的条码等信息，如图 8-475 所示。



图 8-475　设备机框上的条码

说明：该种方式下增加虚拟 CPE，acs 用户名以及密码必须同设备上配置的 cwmp acs username 以及 cwmp acs password 一致，否则可能会存在 CPE 无法自动识别的情况。

如选择了图 8-474 中的快速增加 CPE，则仅需输入 CPE 设备的 OUI 以及序列号即可，acs 用户名以及密码信息，则调用 BIMS 系统参数中的配置，本文不再赘述。

登录 iMC 首页，依次单击"业务"→"分支网点管理"→"配置管理"→"部署向导"→"自动部署 CPE 配置"→"按 CPE"命令，填写相关参数后，如图 8-476 所示。



图 8-476　填写相关参数

单击“下一步”按钮，输入配置模板中的变量 sysname 的值即可，如图 8-477 所示。

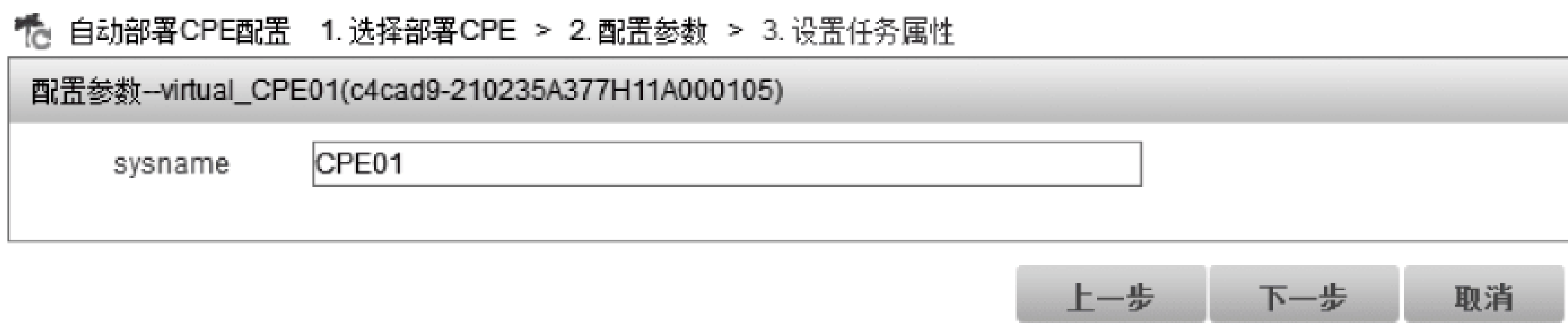


图 8-477　输入配置模板变量 sysname 的值

依次根据部署指导单击“确认”按钮即可创建该任务。

(4) CPE 设备侧 TR-069 配置

CPE 设备侧 TR-069 主要配置如下。

```
#
cwmp
cwmp acs url http://192.168.1.10:9090
cwmp acs username imcbims
cwmp acs password imcbims
cwmp cpe inform interval enable
cwmp cpe inform interval 60
cwmp cpe wait timeout 100
cwmp cpe username cpe
cwmp cpe password cpe
cwmp cpe connect interface Vlan-interface1
#
```

上述命令配置的具体含义请参考相关产品的配置手册，本文不再赘述。

说明：

① cwmp cpe username/passworf 命令配置内容主要为 ACS 向 CPE 主动发起连接时验证所用，如无该需求，该配置可以省略。

② 在 iMC 首页依次单击“业务”→“分支网点管理”→“系统配置”→“系统参数”命令，通用密码状态选择启用且未配置虚拟 CPE 时，cwmp acs username 无实际意义。该处通用密码需要与 cwmp acs password 配置一致。

③ 其他配置参数可随现场环境做适当调整。

(5) DHCP Option 43 属性配置

DHCP Option 43 属性主要用于 DHCP 服务器在 CPE 获取 IP 地址时附带 TR-069 配置信息。该配置在 H3C 设备和其他 DHCP 服务器均可实现，本文以 H3C 设备为例，配置过程有 acs URL Option 43 转换以及 H3C 设备 DHCP 服务器配置。

登录 iMC 首页，依次单击“业务”→“分支网点管理”→“系统配置”→“Option 工具”命令，填写 ACS 的 URL 以及 ACS 用户名密码信息，单击“转换”按钮即可将这类信息转换为 Option 43 属性字段，如图 8-478 所示。

登录 H3C 设备 CLI 命令行，配置内容如下。

```
#
dhcp server ip-pool tr-069
network 172.16.0.0 mask 255.255.255.0
gateway-list 172.16.0.1
```

```
option 43 hex 01286874 74703A2F 2F313932 2E313638 2E312E31 323A3930 39302069 6D636269
6D732069 6D636269 6D73
#
Return
```



图 8-478 “Option 工具”

(6) CPE 设备获取 IP 地址/CWMP 配置

BIMS 零配置场景下，CPE 设备加电启动之后，会自动向 DHCP 服务器获取 IP 地址信息，本例中 CPE 设备分别执行 display ip interface brief 以及 display cwmp status 可查看设备地址获取情况以及 CWMP 学习情况如图 8-479 所示。

```
[CPE]display ip interface brief
*down: administratively down
(s): spoofing
Interface                     Physical Protocol IP Address      Description
GigabitEthernet2/0/1          down     down     2.3.0.2         GigabitEt...
GigabitEthernet2/0/2          down     down     1.2.0.2         GigabitEt...
GigabitEthernet2/0/32         down     down     unassigned      GigabitEt...
GigabitEthernet2/0/47         down     down     unassigned      GigabitEt...
GigabitEthernet2/0/48         down     down     192.168.0.2     GigabitEt...
LoopBack0                     up       up(s)    2.2.2.2         LoopBack0...
Vlan-interface1               up       up       172.16.0.2      Vlan-inte...
[CPE]display cwmp status

TR-069 is enabled.
ACS URL                             :http://192.168.1.12:9090
ACS information is set by           :DHCP
ACS username                        :imcbims
ACS password                        :imcbims
Connection status                   :disconnected
Data transfer status                :none
Time of last successful connection  :2000-04-26T14:42:26
Interval upon to next connection    :303s
```

图 8-479 CPE 设备获取 IP 地址/CWMP 配置

(7) iMC BIMS 是否添加 CPE

iMC BIMS 默认将向其发起加入请求的 CPE 设备添加到本地 CPE 设备列表中。

正常情况下，在非 BIMS 零配置场景中，做了如上配置之后，在 BIMS“所有 CPE”中可以查看到已经成功发现相关 CPE 设备，如图 8-480 所示。

如果未自动发现该 CPE 设备，请参考本流程后续步骤。

在 BIMS 零配置场景下，则可以看到先前创建的虚拟 CPE virtual_CPE01 以及成功添加于 BIMS 中，如图 8-481 所示。

在 CPE 设备上不断查看 CWMP 状态，则可以看到 CPE 设备 sysname 名称已经变化，如图 8-482 所示。



图 8-480　查看已经成功相关 CPE 设备



图 8-481　BIMS 零配置场景

```
[CPE-Vlan-interface1]dis cwmp sta
[CPE-Vlan-interface1]dis cwmp status

TR-069 is enabled.
ACS URL                                :http://192.168.1.12:9090
ACS information is set by              :DHCP
ACS username                           :imcbims
ACS password                           :imcbims
Connection status                      :connected
Data transfer status                   :none
Time of last successful connection     :2000-04-27T12:00:35
Interval upon to next connection       :585s

[CPE-Vlan-interface1]dis cwmp status

TR-069 is enabled.
ACS URL                                :http://192.168.1.12:9090
ACS information is set by              :DHCP
ACS username                           :imcbims
ACS password                           :imcbims
Connection status                      :connected
Data transfer status                   :none
Time of last successful connection     :2000-04-27T12:00:35
Interval upon to next connection       :584s

[CPE01-Vlan-interface1]dis cwmp status

TR-069 is enabled.
ACS URL                                :http://192.168.1.12:9090
ACS information is set by              :DHCP
ACS username                           :imcbims
ACS password                           :imcbims
Connection status                      :connected
Data transfer status                   :none
Time of last successful connection     :2000-04-27T12:00:35
Interval upon to next connection       :583s

[CPE01-Vlan-interface1]
[CPE01-Vlan-interface1]
```

图 8-482　CPE 设备 sysname 名称变化

如果未自动发现该虚拟 CPE 设备或者配置推送失败，请参考本流程后续步骤。

(8) iMC BIMS 进程是否运行正常

在前述步骤都正确的情况下，可能出现 BIMS 未正确识别 CPE 的情况，其中可能的原因之一便是 BIMS 进程本身运行异常。

在 BIMS 服务器侧执行 netstat -aon | findstr 0.0.0.0:9090 便可检测该端口的占用情况，如图 8-483 所示。



图 8-483　端口占用情况

以本例为例，通过任务管理器中查看进程 PID 4644 对应的进程是否为 java.exe 即可。

也可以通过查看部署监控代理中 bimsserver.exe 进程是否运行正常来判断 BIMS 系统是否运行正常。

(9) BIMS 进程问题排查/日志收集

某些情况下，iMC 部署监控代理中 bimsserver.exe 进程无法启动，提示“Web 服务端口已经被其他程序占用。”，如图 8-484 所示。

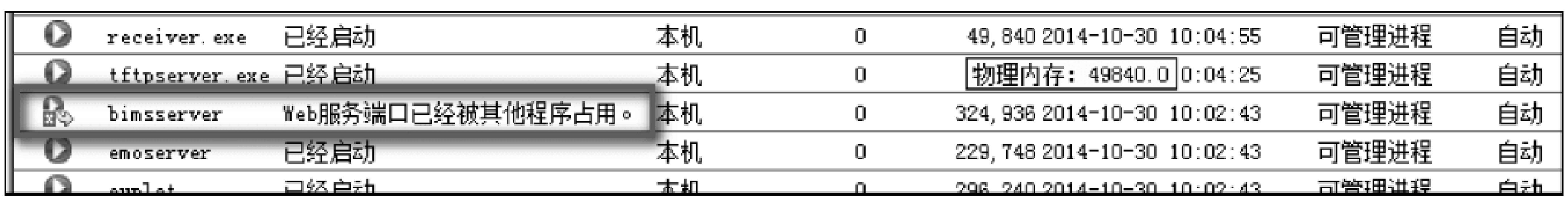


图 8-484　Web 服务端口已经被其他程序占用

查询占用 9090 端口的进程后，发现该端口被 iNodeMngChecker.exe 进程占用，如图 8-485 所示。



图 8-485　查询占用 9090 端口的进程

出现该问题的原因为 iNode 管理中心和 BIMS 服务器部署在同一台物理服务器，所以在日常开局中，尽量避免出现该问题。

如果端口未被占用而 bimsserver.exe 进程仍未启动，则可能存在无法连接数据库等其他原因，针对此类问题，请反馈 iMC PLAT 版本信息、BIMS 版本信息以及\iMC\server\conf\log 目录下 bimsdm.log 和 imcbimsdm.txt 日志。

(10) iMC BIMS 服务器防火墙是否关闭

某些情况下，bimsserver.exe 进程运行正常，但仍可能出现 BIMS 未正确识别 CPE 的情况。可以通过在 CPE 侧 telnet BIMS 服务器 9090 端口来测试 CPE 侧到 BIMS 的防火墙情

况，如果 telnet 显示如下，则认为网络无问题。

```
<CPE>telnet 192.168.1.12 9090
Trying 192.168.1.12 ...
Press CTRL+K to abort
Connected to 192.168.1.12 ...HTTP/1.1 400 Bad Request
Content-Length: 0
Connection: close
Server: Jetty(9.1.4.v20140401)
```

如果 telnet 显示如下，则认为网络中存在防火墙。

```
The connection was closed by the remote host!
<CPE>telnet 192.168.1.12 9090
Trying 192.168.1.12 ...
Press CTRL+K to abort
Failed to connect to the remote host!
```

（11）关闭 iMC BIMS 服务器防火墙或者端口放通

本步骤为日常的网络排错操作，防火墙检查涉及 BIMS 操作系统防火墙以及网络中防火墙策略，本文不再赘述。

（12）TR-069 报文是否正常/内容正确

在极少情况下，可能有 CPE 设备上送给 BIMS 服务器 TR-069 报文异常导致 CPE 设备无法添加的情况。报文异常可能有 TR-069 未携带 OUI 或未携带设序列号导致。图 8-486 所示为日常问题处理中见到的一个报文异常范例抓包，抓包中 TR-069 报文缺失设备序列号，与本文中所涉及的实验无关。

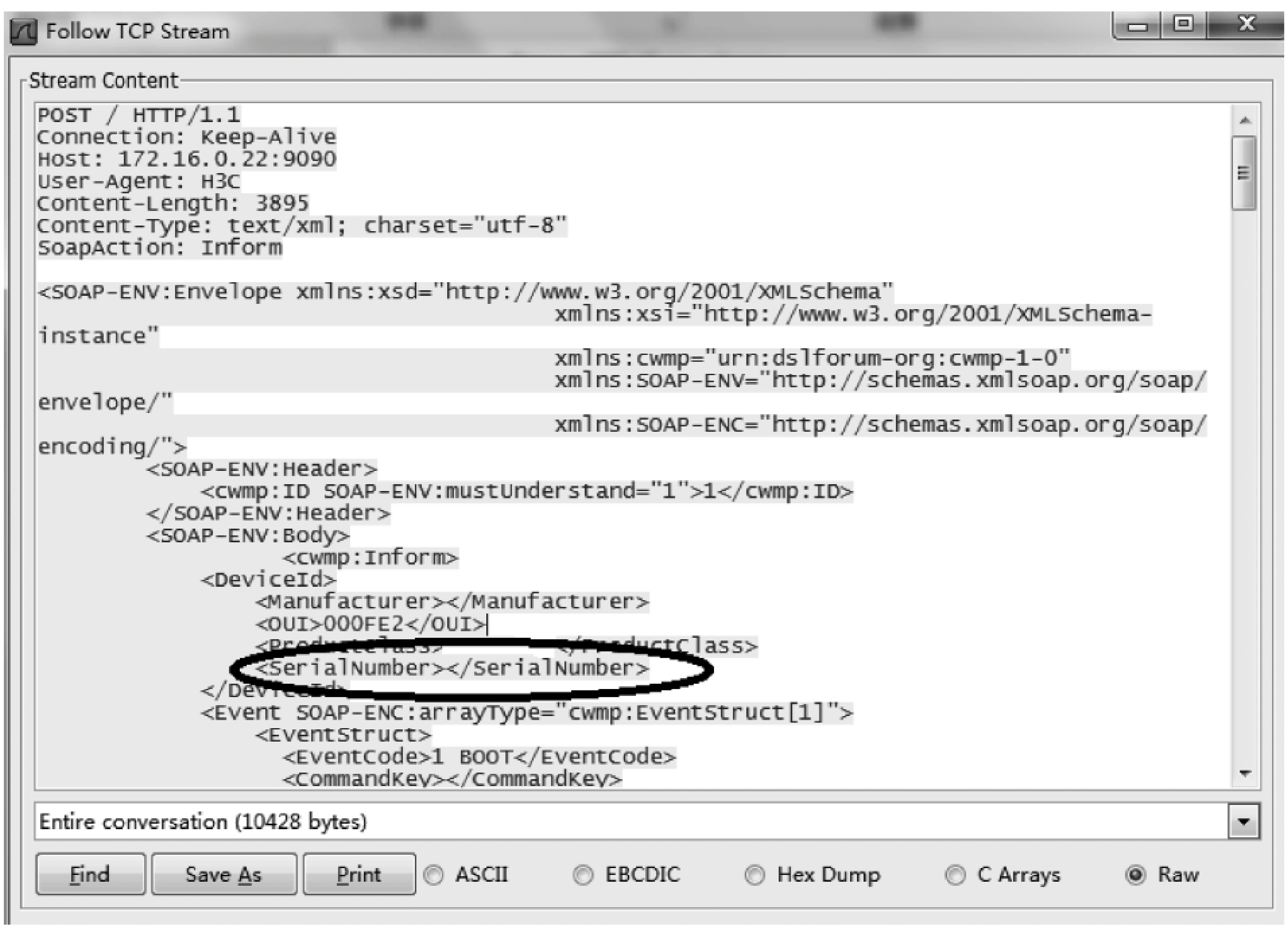


图 8-486 报文异常范例抓包

(13) 抓包收集/日志收集

步骤(12)中所述问题的出现概率极小且较难判断,一般情况下需要提供抓包、iMC PLAT 版本信息、BIMS 版本信息以及\iMC\server\conf\log 目录下 bimsdm.log 和 imcbimsdm.txt 日志。

bimsdm.log 以及 imcbimsdm.txt 日志建议为 DEBUG 级别,日志级别调整须在 BIMS 系统参数配置中将 ACS 运行日志调整为 DEBUG,如图 8-487 所示。

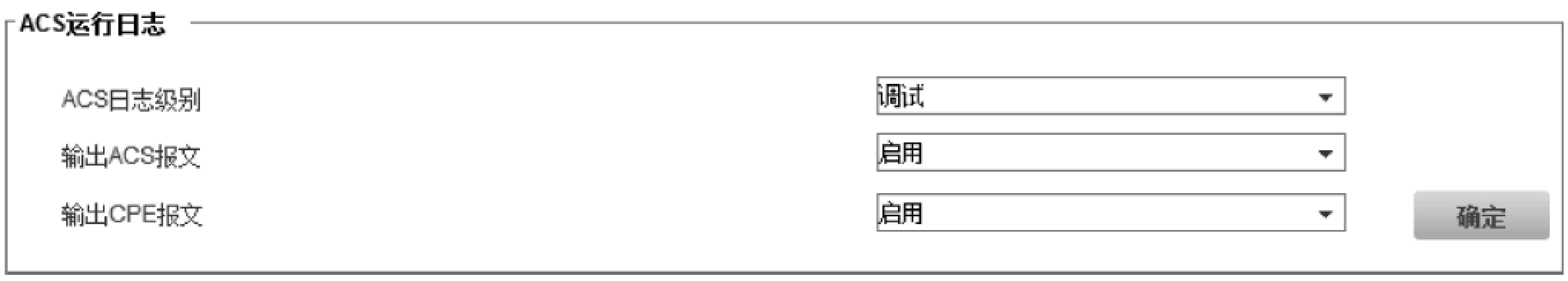


图 8-487 ACS 运行日志调整

(14) 配置是否推送到 CPE/BIMS 页面操作 CPE 是否成功

该类问题常见于非 BIMS 零配置场景,在 BIMS 页面针对 CPE 做某些操作以及将配置推送到 CPE 设备本质相同,本例中就合二为一分析。出现该类问题可能原因较多,请参考后续问题处理步骤。

(15) CPE 设备类型是否为 NAT 设备

BIMS 与 CPE 设备之间建立连接主要有两种方式:一是 CPE 发送 inform 报文与 BIMS 侧的 TCP 9090 端口发起连接。二是 BIMS 发送 inform 报文与 CPE 侧的 TCP 7547 端口发起连接。正是由于方式一的场景,才使得 BIMS 可以管理 NAT 内网的 CPE 设备。

当设备实际为 NAT 设备时,由于路由协议等本身的限制,BIMS 是无法立即向 CPE 推送配置的。所以设备实际上是否为 NAT 设备,对 BIMS 向设备推送配置/操作等动作也是有很大的影响。

(16) iMC BIMS 侧 CPE 设备类型是否显示正确

某些情况下,设备实际上为非 NAT 设备,但在 BIMS 侧却显示为 NAT 设备,该问题会对 BIMS 日常的使用造成影响,要想解决该问题请参考步骤(17)。

(17) CPE 设备侧 TR-069 配置优化

BIMS 判断设备是否为 NAT 设备主要依据 TR-069 报文中的源 IP 地址以及报文载荷中的 CPE URL 信息。当报文源 IP 地址和 URL 中 IP 地址信息不一致时,BIMS 判断该设备为 NAT 设备,当二者信息一致时,BIMS 判断设备为非 NAT 设备。

默认情况下,系统会采用一定的机制去获取一个 CWMP 连接接口,可能存在该 CWMP 链接接口地址与报文源 IP 地址不一致的情况,在此情况下,需要指定 CPE 侧 CWMP 连接接口,具体命令如下。

```
[CPE-cwmp]cwmp cpe  connect interface XXX
```

(18) 配置部署调度方式修改

BIMS 部署任务的调度方式分为立即执行、定时执行以及尽快执行。当 CPE 设备为 NAT 设备时,连接的发起方为 CPE 设备,所以调度方式为立即执行或定时执行可能会导致任务部署失败,需要将任务的调度方式调整为尽快执行,如图 8-488 所示。



图 8-488　配置部署任务调度方式修改

(19) iMC BIMS 与 CPE 非 NAT 类型情况下是否互通

在非 NAT 环境下，BIMS 向设备推送配置失败的原因可能有 BIMS 无法主动与设备建立连接，该种情况下，BIMS 的打印出如下内容。

```
2014-11-02 16:37:30 [ERROR] [bimsSenConnectionRequestTaskExecutor-1] [com.imc.bims.acs.commons.HTTPUtils::sendConnectionRequest] Connect to http://172.16.0.2:7547/cpe fail, user=, pwd=, IOException.
2014-11-02 16:37:30 [ERROR] [bimsSenConnectionRequestTaskExecutor-1] [com.imc.bims.acs.task.func.TaskMgrImpl $ 1::run] Create task exception: com.imc.bims.commons.AcsException: Connection to http://172.16.0.2:7547 refused
  2014-11-02 16:37:30 [DEBUG] [bimsSenConnectionRequestTaskExecutor-1] [com.imc.bims.acs.task.func.TaskMgrImpl $ 1::run] Create task exception:
  com.imc.bims.commons.AcsException: Connection to http://172.16.0.2:7547 refused
```

从部署任务的页面报错也可以看到类似如图 8-489 所示信息。



图 8-489　页面报错

出现该中情况的主要原因有三点：一是网络中存在防火墙，未放通 BIMS 至 CPE 侧的 TCP 7547 端口。二是设备本身 CWMP 由于某种原因关闭，在 CWMP 视图下配置 cwmp enable 即可。三是 BIMS 侧和设备侧的 CPE 用户名密码配置不一致。由于出现该种情况的场景排查较为简单，本文不再赘述。

(20) BIMS 服务器是否开启 IPv6 协议栈

BIMS 目前不支持 IPv6 协议，如果服务器有多个网卡且使能 IPv6 协议，则可能出现对 CPE 进行操作提示超时的现象，出现该问题请参考步骤(21)。

(21) 卸载 IPv6 协议栈/BIMS 配置文件修改

请禁止使能服务器网卡的 IPv6 协议。

如果客户现场有 IPv6 业务无法禁用 IPv6 协议，则可以通过修改 BIMS 后台配置文件规避，具体内容如下。

修改文件包括：

```
iMC\client\conf\bimsmsgcomm.properties
修改#msg.master.addr = 192.168.1.10
为 msg.master.addr = 127.0.0.1                //该地址为 127.0.0.1
iMC\server\conf\bimsserver.properties
修改#msg.master.addr = 192.168.1.10
为 msg.master.addr = 127.0.0.1                //该地址为 127.0.0.1
修改#msg.slave.addr = 192.168.1.10
为 msg.slave.addr = 127.0.0.1
//msg.slave.addr 地址为 BIMS 部署地址，如果为集中式，则为 127.0.0.1
```

(22) 是否备份 CPE 设备配置

CPE 设备配置备份为 BIMS 常用功能之一，操作员创建备份配置任务，系统会按照执行周期定时执行备份，操作员也可以根据需要立即执行备份。调度方式分为立即、定时和周期性执行。

(23) 备份 CPE 设备配置

登录 iMC 首页，依次单击“业务”→“分支网点管理”→“配置管理”→“CPE 配置备份”→“增加 CPE 配置备份任务”命令，填写相关参数之后便可成功创建一设备配置备份任务，如图 8-490 所示。



图 8-490　备份 CPE

说明：设备类型为 NAT 设备时请选择尽快执行，一般情况下我们也建议执行方式配置为尽快执行。

(24) CPE 设备配置是否备份成功

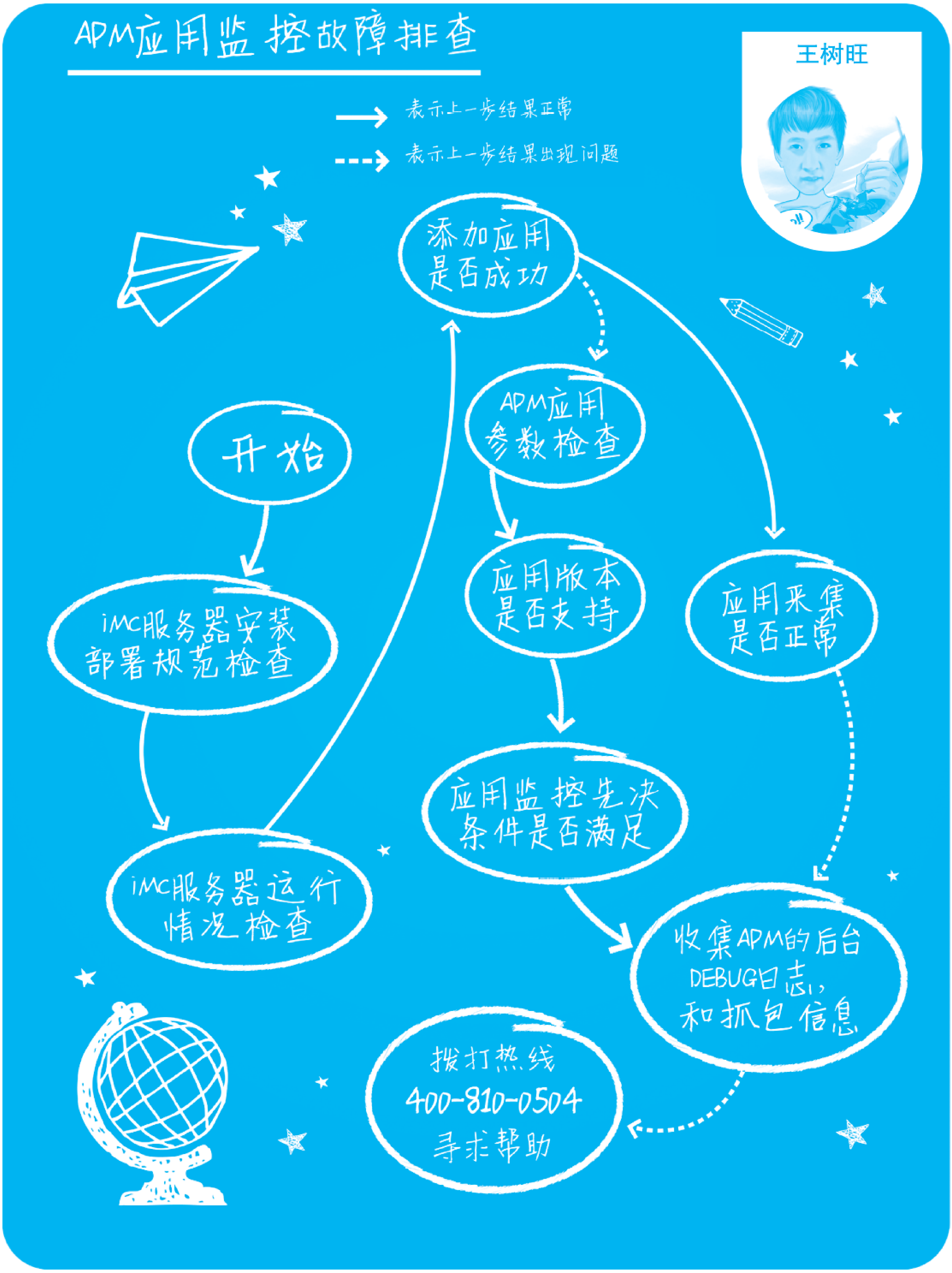
可以在单击“业务”→“分支网点管理”→“备份历史记录”→“backup01”命令后查看备份任务的执行情况，本例中 CPE 设备配置备份成功，如图 8-491 所示。

(25) 抓包收集/日志收集

如果 CPE 配置备份失败，请确认设备上是否配置 ip http enable。如果已经配置，请提供抓包、iMC PLAT 版本信息、BIMS 版本信息以及\iMC\server\conf\log 目录下 bimsdm.log 和 imcbimsdm.txt 日志。



图 8-491 CPE 设备配置成功与否


APM应用监控故障排查
王树旺
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
添加应用是否成功
APM应用参数检查
应用版本是否支持
应用监控先决条件是否满足
应用采集是否正常
收集APM的后台DEBUG日志，和抓包信息
拨打热线 400-810-0504 寻求帮助

1. 开始

随着 Web 2.0、云计算、数据中心等信息技术的不断发展，企业的各种业务已经越来越紧密地与 Internet 结合在一起，由服务器、数据库、中间件等组成的应用信息系统也变得越来越复杂，对 IT 技术人员的要求也越来越高，各种突发故障排除起来也越来越困难。因此企业急需一套易于部署、功能全面、扩展灵活的 IT 运维管理解决方案，满足其不同层次的应用管理需求。

APM 应用监控排错的基本思路：APM 是管理服务器、数据库、中间件等应用信息的综合监控系统，其中最重要的是通过监控协议获取应用的数据信息；不同的应用需要对应不同的监控协议，针对不同的应用，我们首先确认对应的监控协议是否正常开启、权限是否足够；然后根据不同应用的监控协议进行检查。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

需要对照《智能管理中心(iMC)部署和硬件配置方案》，检查 iMC 服务器性能是否符合配置要求。该配置是我们推荐的运行 iMC 最基本的部署要求，请严格执行。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果 APM 监控的应用数量多，需考虑是否根据《智能管理中心(iMC)部署和硬件配置方案》要求将组件分布式部署在性能良好的服务器上，重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统和数据库是否为 64 位，建议使用 64 位系统。

② 单击“开始”→“智能部署监控代理”命令，选择“部署”标签，检查“APM(应用管理)”是否已经部署，如图 8-492 所示。



图 8-492 检查“APM(应用管理)”已部署

说明：

(a) APM默认的采集间隔是5分钟，最多支持500个应用监控，如果不采用5分钟的采集间隔，管理规模需要相应调整，例如：采集间隔调整为10分钟，则管理规模也将加倍。

(b) 当基础版本为iMC APM 7.0 (E0201)时，APM Agent只支持手动升级。

(2) iMC服务器运行情况检查

要想正常增加应用和正常监控应用数据，必须确保APM功能模块对应的imcapmedm进程运行正常。

单击"开始"→"智能部署监控代理"命令，选择"进程"标签，查看APM的进程imcapmedm是否正常启动，具体如图8-493所示。



图 8-493　进程启动情况

说明：一般情况下，这些进程通过鼠标右键设置启动方式为"自动启动"。

(3) 添加应用是否成功

APM应用添加成功状态如图8-494所示。



图 8-494　APM应用添加成功状态

APM 应用添加失败状态如图 8-495 所示。

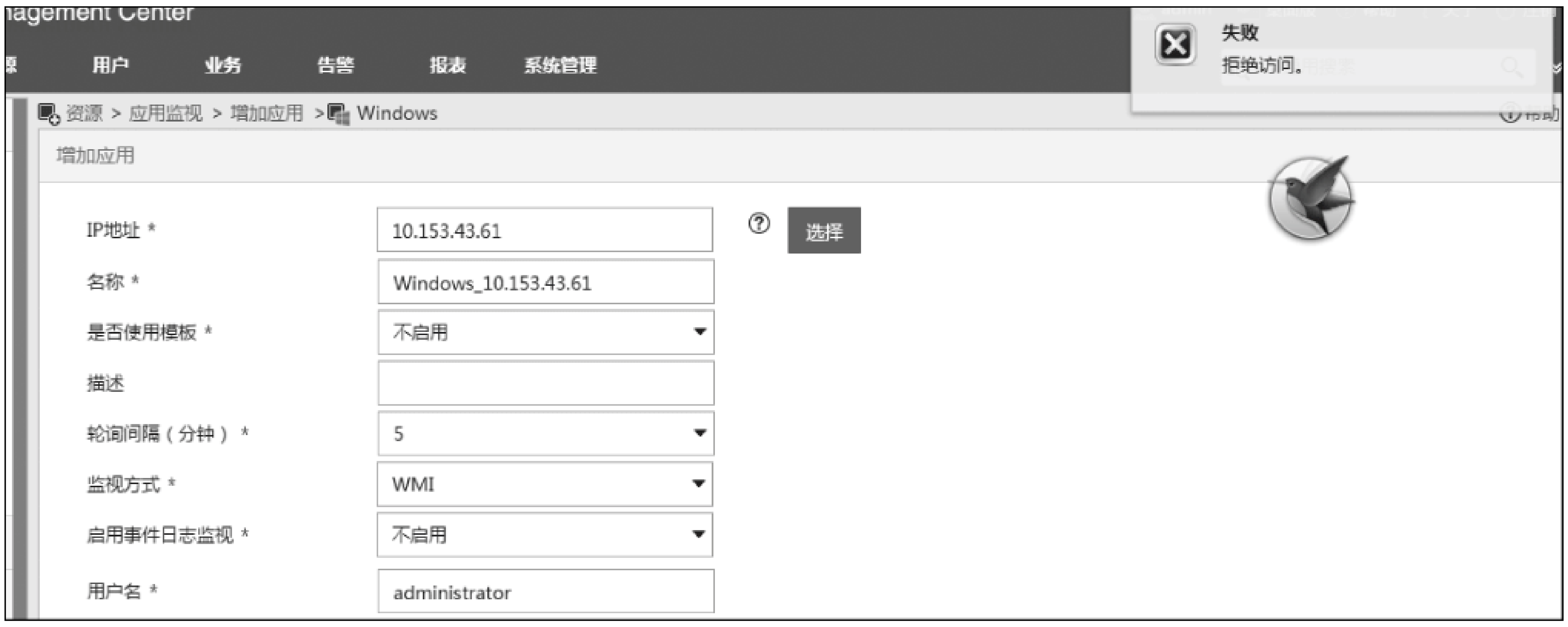


图 8-495　APM 应用添加失败状态

(4) APM 应用参数检查

为了成功监控 APM 应用信息，APM 不同的应用监控的方式和支持版本均不一致；在 APM 增加应用监控失败场景需要从如下几方面进行排查。

① 应用版本支持情况检查。

不同的应用 APM 支持的版本也是有限制的，需要再增加前首先确认应用的版本是否在 APM 适配范围内。版本适配范围在增加界面的帮助中可以查看，如图 8-496 所示。

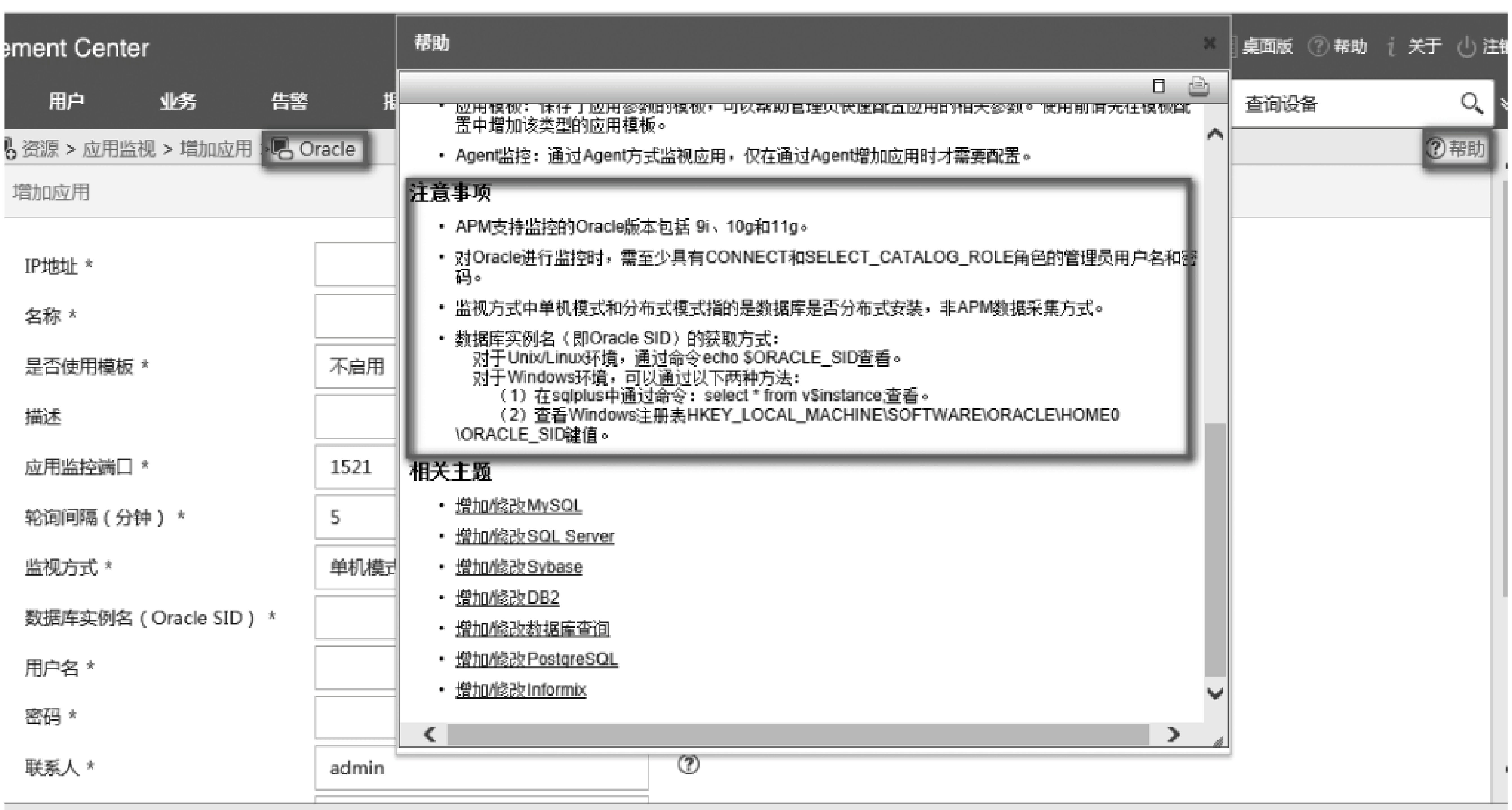


图 8-496　增加页面的帮助

② 应用监控先决条件检查。

常见的应用如：Windows 应用，通过 WMI 方式监控，需要 Windows 服务器开启 WMI 协议，并使用管理员权限账号增加监控。服务器 WMI 服务开启确认方式如图 8-497 所示。

测试账号是否有权限，可以通过最常见的方式，即从 APM 服务器上通过远程桌面的方式登录 Windows 服务器，查看是否有权限登录。

注意事项

- 采用WMI方式对Windows服务器进行监控时，需要具有管理员权限的用户名和密码。
- 当应用管理组件部署在Windows Server 2008系统上时，不能监控Windows Server 2003系统。
- 只有WMI方式能够监控事件日志，SNMP方式无法监控事件日志。
- 当试图通过WMI模式添加应用时，提示"拒绝访问。"，处理办法参见常见问题解答。
- 当使用Linux平台的APM监控Windows Server 2008 或 Win 7时，处理办法参见常见问题解答。
- 如果通过SNMP方式监控服务器，服务状态只能获取正在运行的状态，其值为1。配置服务状态阈值时，请配置1，表示"正在运行"。
- 如果通过WMI方式监控服务器，配置服务状态阈值时，请配置如下值：ContinuePending、Paused、PausePending、Running、StartPending、Stopped、StopPending，分别表示"正在恢复"、"已暂停"、"正在暂停"、"正在运行"、"正在启动"、"已停止"、"正在停止"。
- 对于系统运行时长指标，以秒为单位配置阈值。
- 当iMC安装在Windows操作系统且Windows应用使用WMI方式监视时，服务启动、停止功能可用。
- 启用事件日志监视后，应用管理会采集指定类型的Windows事件日志。当事件日志条数超过事件日志告警阈值所指定的条数时，应用管理只采集阈值指定条数的事件日志并产生相应的告警信息。该告警不影响Windows应用的健康状况。
- 在Linux环境下，添加Win2012应用之前，该监控的主机必须开启'Remote Registry'服务。
- 监视Windows Server 2008及后续版本的Windows应用时，必须使用Windows应用的administrator用户。

图 8-497　服务器 WMI 服务开启确认方式

另外，针对不同的应用，在 APM 的帮助中注明了增加监控的先决条件，需要现场逐一排查。

（5）应用采集异常

在 APM 的应用监控中，如果应用监控状态为"不可用"或"无法访问"时，该应用不能正常采集，如图 8-498 所示。

	名称	应用类型	速率(bps)	流量(H)	流量(D)	可用性	健康状况	管理状态	相关应用	修改	删除
	Apache_10.153.49.77	Apache服务器	-	-	-	不可用	紧急	管理			
	CAS_172.16.0.201	CAS	-	-	-	无法访问	--	管理			
	MSSQL_10.153.43.100	SQL Server	-	-	-	可用	健康	管理			

图 8-498　应用采集异常

（6）APM 应用增加失败和获取数据异常定位信息收集

现场经常会出现，权限配置检察没有问题，按照帮助排查未能解决现场问题时，就需要按照要求收集后台的 DEBUG 日志和抓包信息来定位问题原因。

① 后台 DEBUG 日志收集方法。

登录 iMC 服务器，进入 APM 所部属的服务器上，进入后台目录：&iMC\server\conf 目录下，用记事本打开 qvdm. conf 文件，找到如下信息，将默认的 INFO 改成 DEBUG 后保存。

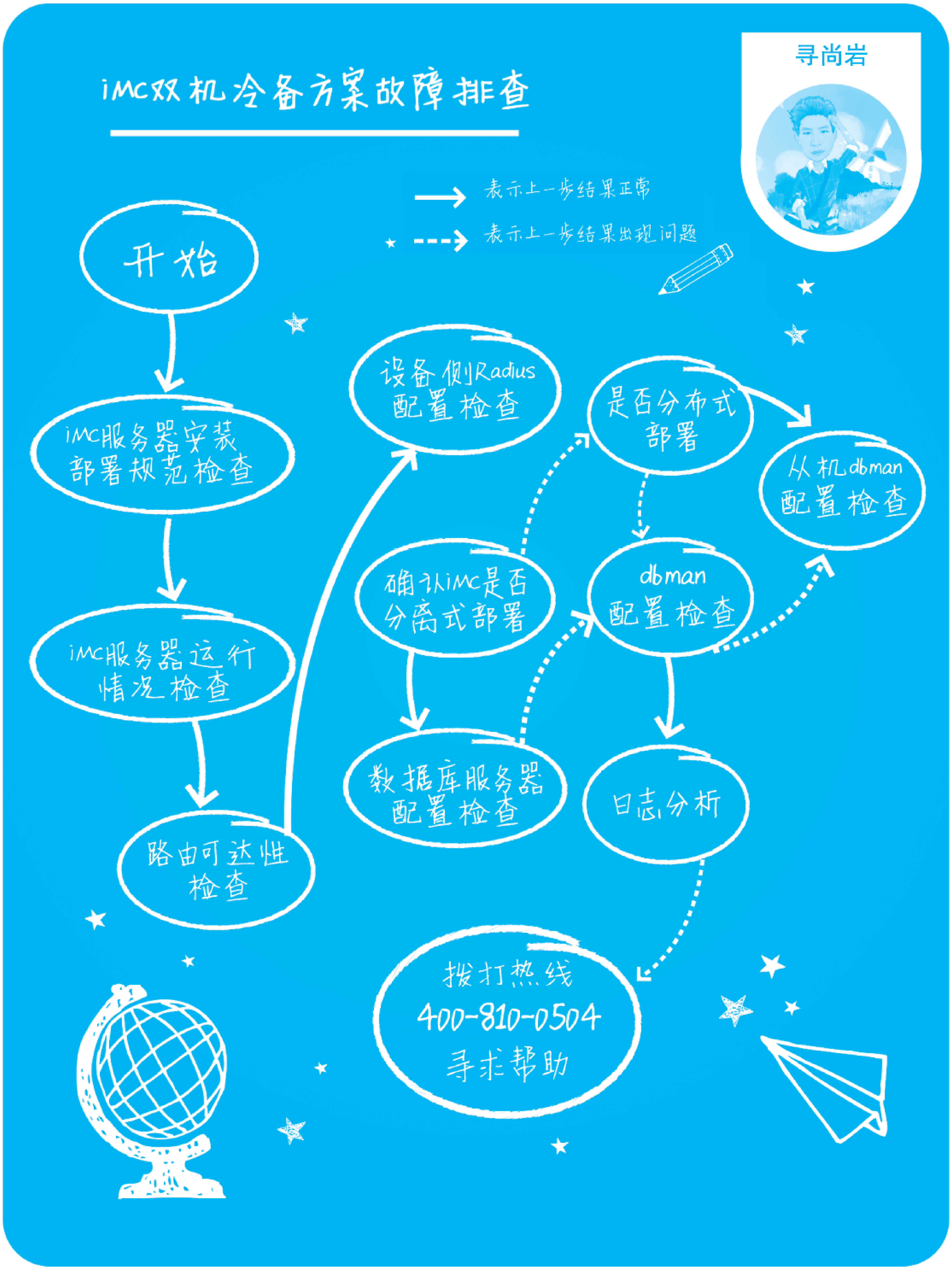
```
#setting log level (DEBUG, INFO, WARNING, ERROR, FATAL)
LogLevel = INFO            //该处将 INFO 改为 DEBUG
#setting log expire (its unit is day)
LogExpire = 15
```

重启智能部署监控代理中的 imcapmedm 进程；然后复现问题，收集 &iMC\server\conf\log 下当天的 imcapmedm 的日志信息，打开看一下是否有 DEBUG 字样信息，并且搜索对应的应用 IP 可以看到增加过程的报错信息。

② 抓包信息收集方法。

在 iMC 的 APM 部署所在的服务器上开启抓包工具，复现问题。停止抓包，保存抓包文件。

说明：以上两个信息同时收集，定位问题需要按照报错时间查看抓包中的报错信息定位。


iMC双机冷备方案故障排查
寻尚岩
表示上一步结果正常
表示上一步结果出现问题
开始
iMC服务器安装部署规范检查
iMC服务器运行情况检查
路由可达性检查
设备侧Radius配置检查
确认iMC是否分离式部署
数据库服务器配置检查
是否分布式部署
dbman配置检查
从机dbman配置检查
日志分析
拨打热线
400-810-0504
寻求帮助

1. 开始

iMC 双机冷备是一种容错方案。该方案要求系统中存在一主、一备两套 iMC，且两套 iMC 部署版本完全一致，两套 iMC 之间通过自带的 dbman 工具实现数据从主 iMC 到备 iMC 的自动同步。主 iMC 系统 down 后，设备会自动转向备用 iMC 认证，切换时间控制在秒级，保证了客户业务的连续性。iMC 冷备方案问题包括认证/切换异常和数据不能自动备份或恢复两方面；对于 iMC 冷备方案定位故障的思路及顺序是：iMC 服务器软硬件状态及路由可达性检查、设备配置检查、确认 iMC/数据库部署方式、数据库服务器配置检查、dbman 配置检查、日志分析。

本文举例组网如图 8-499 所示。

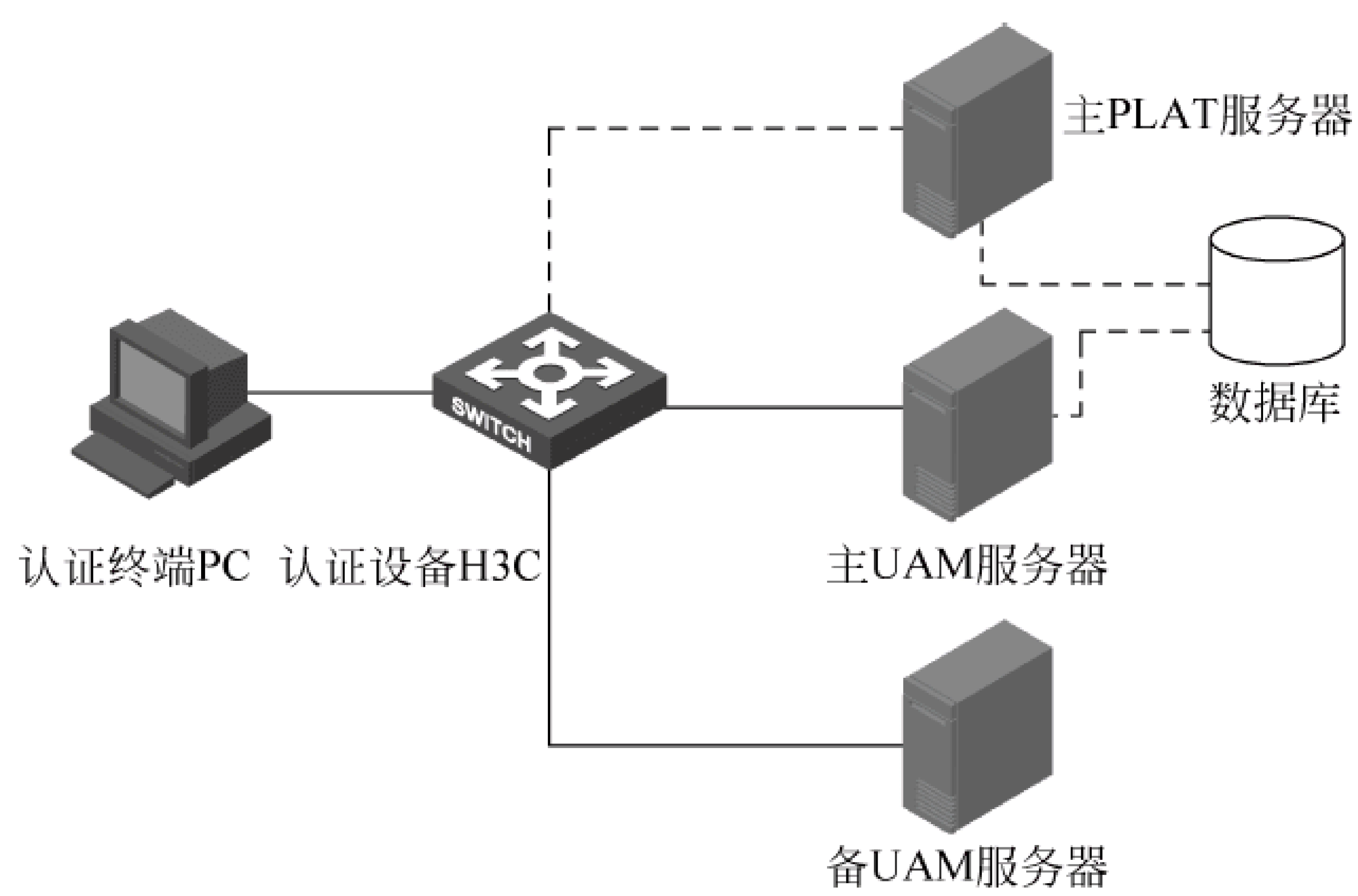


图 8-499 组网举例

IP 规划如下。

认证终端 PC：172.16.16.2/24，网关 172.16.16.1。

认证设备：VLAN 16：172.16.16.1/24，VLAN 100：172.16.100.1/24。

主 PLAT iMC 服务器：172.16.100.122/24，网关 172.16.100.1。

主 UAM 服务器：172.16.100.123/24，网关 172.16.100.1。

数据库服务器：172.16.100.124/24，网关 172.16.100.1。

备 iMC 服务器：172.16.100.125/24，网关 172.16.100.1。

虚线表示分布式或分离式部署。

2. 流程图相关操作说明

(1) iMC 服务器安装部署规范检查

服务器性能是保证 iMC 认证系统稳定运行的基本要素，所以排查问题是首先需要确认服务器软硬件配置情况。

请对照《智能管理中心(iMC)部署和硬件配置方案》查询这套 iMC 服务器的业务量是否符合配置要求。该配置方案是我们推荐的运行 iMC 最基本的部署要求。

① 对照《智能管理中心(iMC)部署和硬件配置方案》检查服务器 CPU、内存、硬盘等是否合乎规格，如果认证数量大、同时在线人数多，则需要根据《智能管理中心(iMC)部署和硬件配

置方案》要求将组件分布式部署在性能良好的服务器上。

重点需要检查内存占用是否过高，内存大小是否满足《智能管理中心(iMC)部署和硬件配置方案》计算出的要求，操作系统是否是高性能的 x64 版本。

② 打开部署监控代理，在部署监控代理中查看部署页面，“用户接入管理”组件是否是“已部署”的状态。

需要关注的组件为“用户接入管理”，其状态应为“已部署”，如图 8-500 所示。



图 8-500　组件部署状态

(2) iMC 服务器运行情况检查

查看主备“iMC 智能部署监控代理”中进程选项卡中是否有未启动的进程，各进程是否正常为“已经启动”。

① 在部署监控代理中，查看 uam.exe、uamjob、ispserver、dbman、policyserver 进程是否正常启动，如图 8-501 所示。

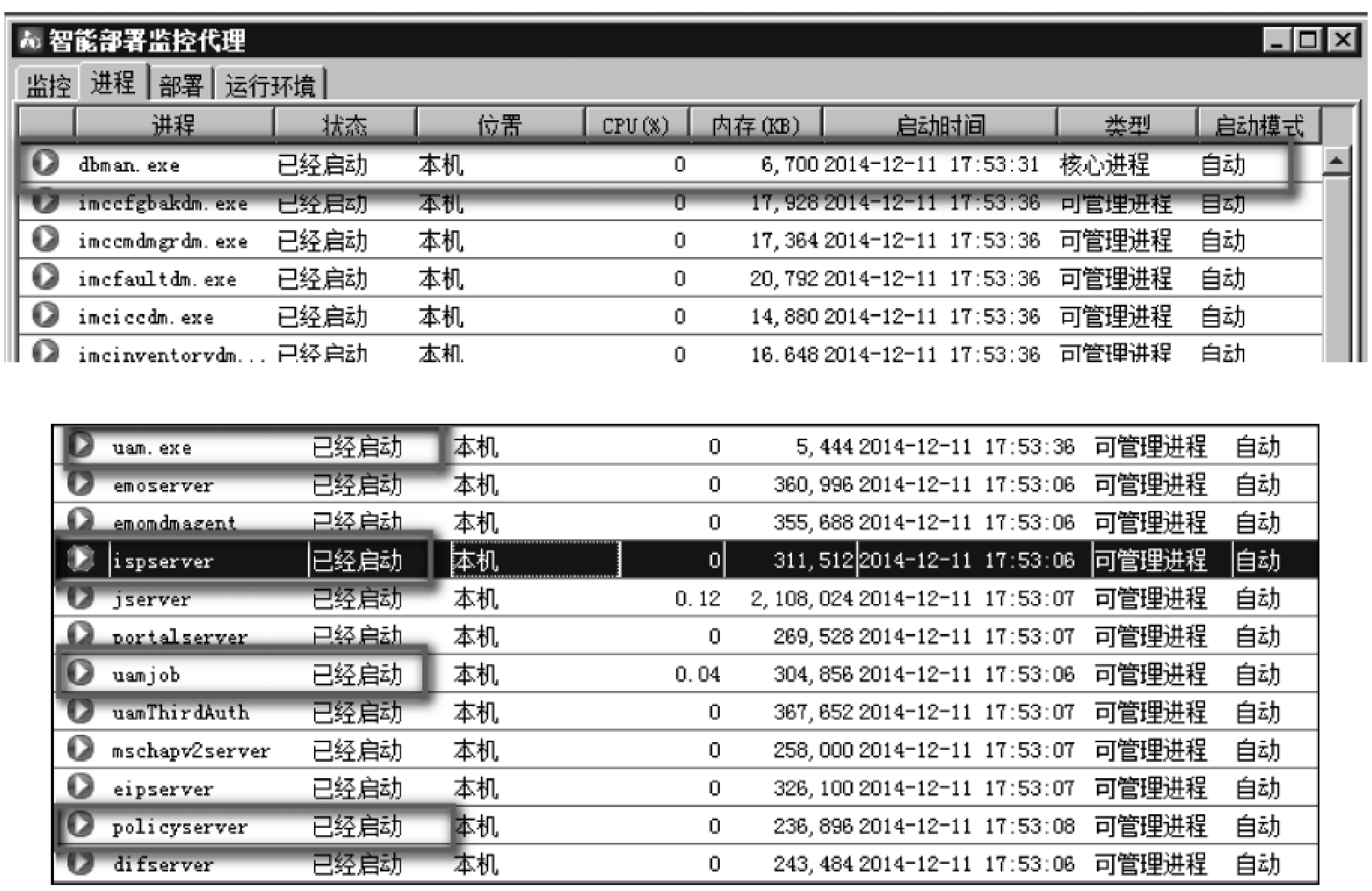


图 8-501　进程启动情况

说明：

(a) 一般情况下，这些进程通过鼠标右键设置启动方式为“自动启动”。

(b) uamjob 功能主要是执行定时任务，uam 进程主要负责认证、计费。

(c) policyserver 主要用来提供客户端类功能。

(d) dbman 提供数据自动备份、恢复功能。

(e) ispserver 统一代理与 iNode 客户端的通信。

② 检查 iMC 服务器 1812、1813 UDP 端口是否被 uam 相关进程所监听，如图 8-502 所示。

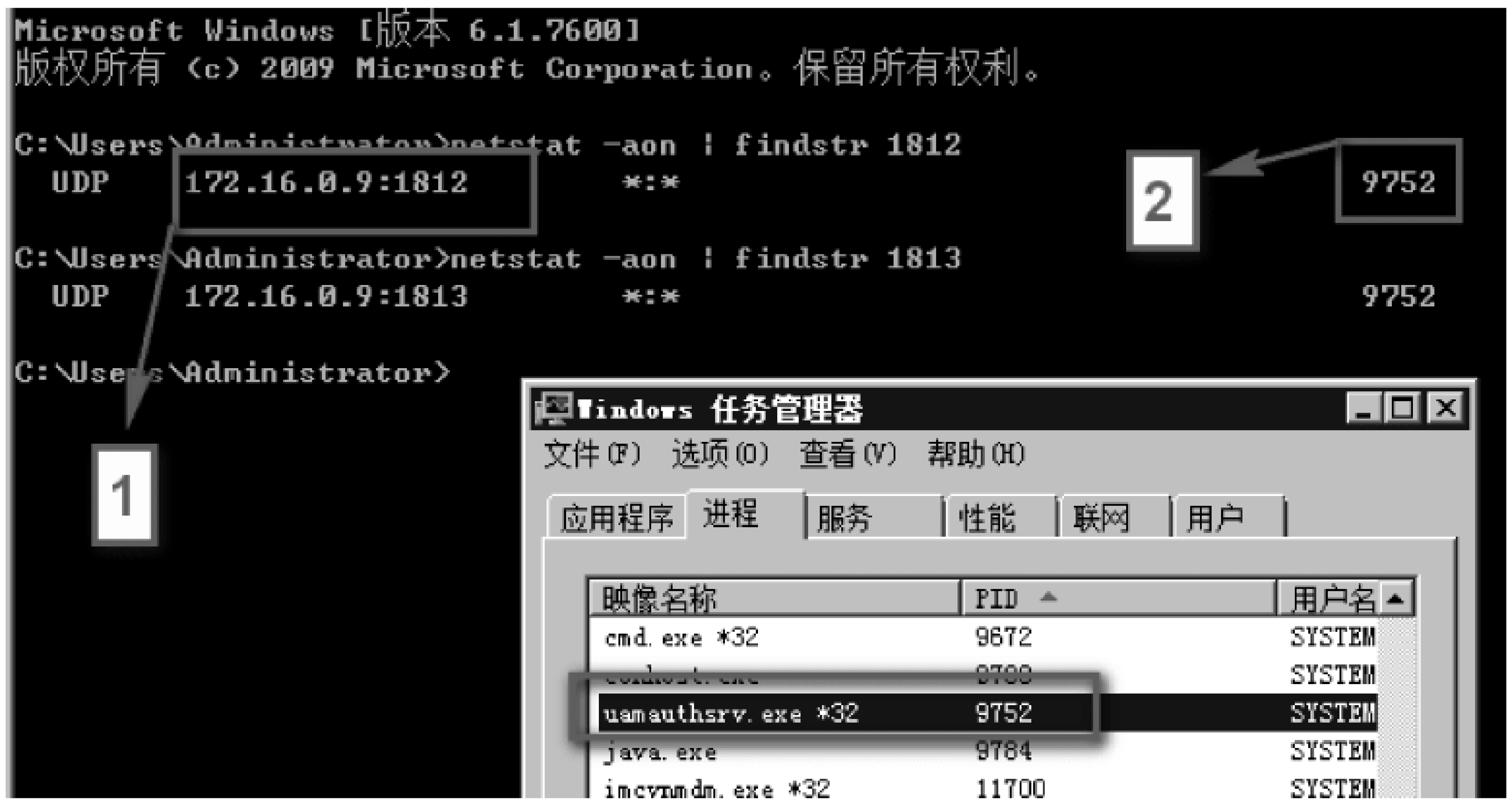


图 8-502　端口被 uam 相关进程监听情况

检查 iMC 服务器 TCP 端口 2810 是否被 dbman 进程监听，如果是分离式部署还需要确认数据库服务器 TCP 端口 2810 是否被 dbman 进程监听，如图 8-503 所示。



图 8-503　TCP 端口 2810 被监听情况

检查服务器 UDP 9019 端口是否被 java 进程监听。

说明：

(a) Windows 操作系统中，通过

netstat -aon | findstr ：端口号

命令来显示某一端口的监听状态及其对应的进程 PID。

(b) 1812、1813 所对应的进程 PID 应为 uam 相关的进程。

(c) 1812、1813 对应的 IP 应为 UAM 服务器实际 IP 地址。

(d) 9019 端口所对应进程 PID 为 policyserver 相关进程。

(e) 2810 端口所应用进程 PID 为 dbman 相关进程。

(f) Linux 系统命令

Netstat -apn | grep 端口号。

③ 检查“iMC 智能监控代理”→“运行环境”选项卡，数据库连接状态是否正常，如图 8-504 所示。

(3) 路由可达性检查

单击“用户”→“接入策略管理”→“接入设备管理”→“接入设备配置”→“增加接入设备”命

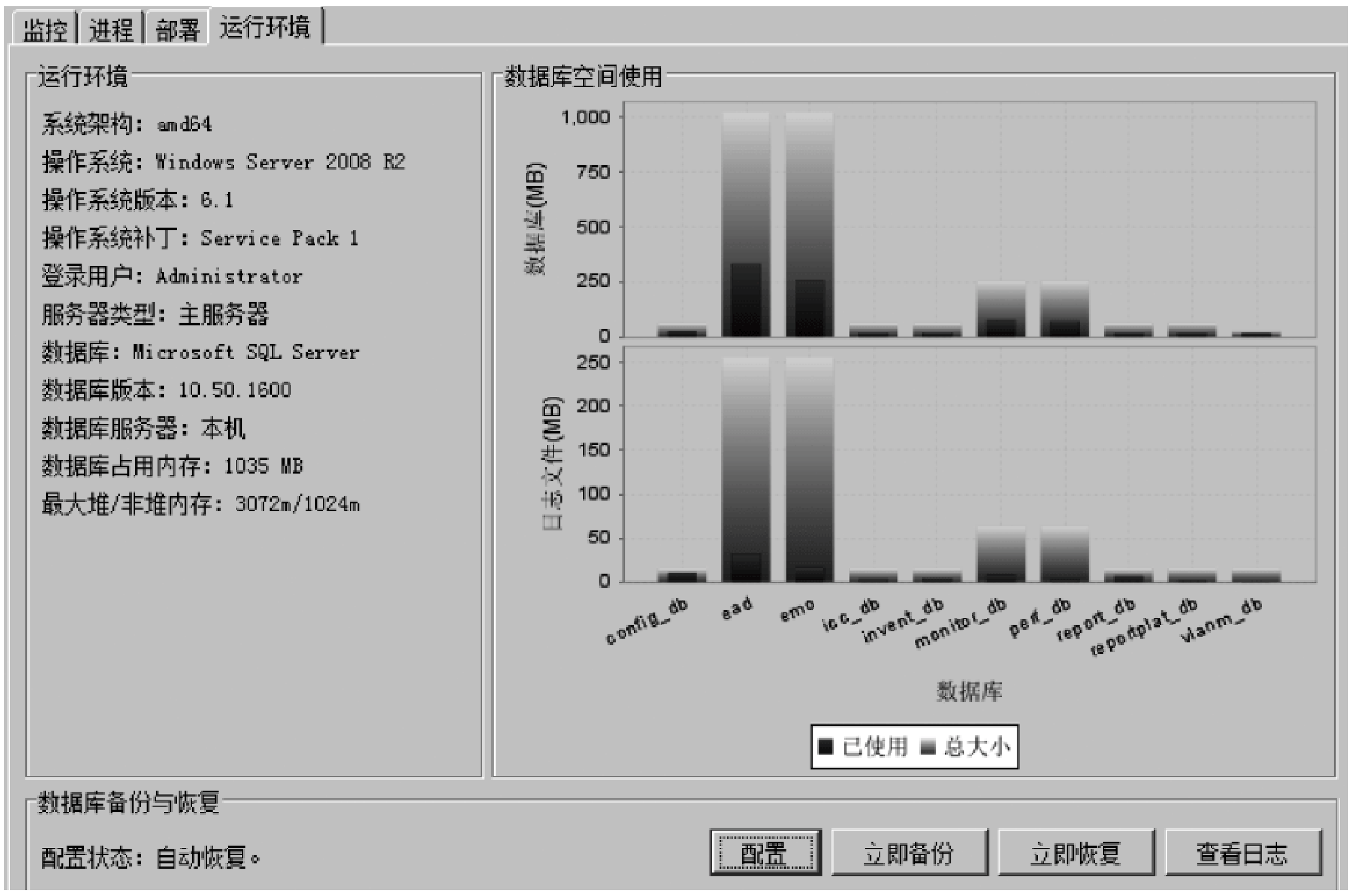


图 8-504 “运行环境”选项卡

令后将需添加接入设备发给 iMC 服务器 Radius 协议报文的端口 IP，iMC 默认会同该 IP 进行 Radius 协议报文交互，需保证 iMC 可以 ping 通该 IP，本例中接入设备 IP 应为 172.16.100.1。

主 iMC 服务器、备 iMC 服务器、数据库服务器间保证路由可达。

说明：

① 接入设备会有多个 IP 地址，如果要更改接入设备 IP，需在 Radius Scheme 视图下配置如下命令。

[sw-radius-h3c] nas-ip 172.16.2.1，并在 iMC 上更改为 172.16.2.1。

② 如果系统开启防火墙，需要放通 TCP 1433 和 2810 端口保证服务器间正常交互数据报文，如图 8-505 所示。



图 8-505 接入设备

(4) 设备侧 Radius 配置检查

```
[BAS-radius-H3C]display this
 radius scheme H3C
 server-type extended
 primary authentication 172.16.100.123
 primary accounting 172.16.100.123
 secondary authentication 172.16.100.125
 secondary accounting 172.16.100.125
 key authentication 123
 key accounting cipher 123
 nas-ip 172.16.100.1
```

说明：

① 接入设备需要配置主备认证、计费服务器，主服务器 down 后，接入设备连续发 3 次请求得不到回应就会自动转向备 UAM 认证。

② 接入设备会将认证、计费分开处理，认证转向备机后，设备仍会将计费报文发往主机，所以主到备切换时第一次会失败，重拨一次即可成功上线。

③ 接入设备重传超时次数由以下参数决定：[BAS-radius-h3c]retry x。

(5) 确认 iMC 是否分离式部署

确认 iMC 组件是否和数据库安装在同一台服务器，如果安装在同一台服务器属于本地数据库；如果是安装在不同服务器属于分离式部署。

(6) 数据库服务器配置检查

① 确认数据库服务器软硬件环境是否满足《硬件配置指导》里面的推荐配置。

② 确认数据库服务器 dbman 进程是否正常运行，TCP 2810 端口(Oracle 对应 1521)是否被 dbman 正常监听。

③ Windows“系统”→“开始”→“管理工具”→“服务”里面，SQL Server(MSSQLSERVER)服务是否是“已启动”状态，正常情况应该显示为“已启动”。Linux 系统可以在 shell 环境下输入如下内容。

```
netstat -anp | grep tnslsnr
netstat -anp | grep oracleorcl
```

判断数据库服务是否正常运行，监听器是否正常监听。

④ 确认数据库配置是否满足《数据库配置指导》里面的要求。

说明：

(a) 对于分离式部署环境，需要在数据库服务器上安装运行 dbman。

(b) Windows 操作系统，需要在数据库服务器上安装 Microsoft Visual C++ 2008 redistributable，该安装程序存放于 iMC 安装盘 Componnents\common\server\vcredist. exe，然后安装 dbman。

(c) Linux 系统，需要设置如下环境变量。

BRARY_PATH= $LD_LIBRARY_PATH:/INSTALL_DIR/dbman/bin。

(d) iMC 部署完成后，需要将 dbman 文件夹拷贝到数据库服务器上并运行，启动如下命令。

```
[root@localhost bin]# cd /opt/iMC/dbman/bin/
[root@localhost bin]# dbman
```

（7）是否分布式部署

检查 iMC PLAT 与各组件之间是否是分布式部署。

（8）从机 dbman 配置检查

V7 版本 iMC 所有的 dbman 配置操作均在主机进行，从机仅需要保证 dbman 进程正常监听 TCP 2810 端口。

说明：从机防火墙需要放开到 TCP 2810 的连接，不然会导致数据传输失败。

（9）dbman 配置检查

① 主 iMC 服务器 dbman 配置示例。

主 iMC 需要选择自动备份模式，如图 8-506 所示。



图 8-506　主 iMC 服务器 dbman 配置示例

每日备份时间点：用于设置每日自动备份的时间点，不建议修改。

备机系统的主机 IP：备用 iMC 服务器的地址，本例为 172.16.100.125。

iMC 服务器地址：127.0.0.1。

数据库地址：集中式部署时填写 127.0.0.1；分离式部署时填写数据库服务器 IP 地址，本例为 172.16.100.124。

备份文件存放路径：本地存放 iMC 数据的路径，名称尽量不要包含中文，且该路径一定要实际存在。

本地备份：勾选表示主机 dbman 会自动备份该数据库。

传送至备机：勾选表示主机 dbman 备份的数据会自动传送至备 iMC 服务器。

说明：

（a）dbman 要求主备 iMC、数据库版本完全一致，否则会导致数据恢复失败。

（b）对于主机有、备机没有的组件，不允许对该组件对应的数据库勾选“传送至备机”。

（c）不建议备份 NTA/UBA/WSM/SYSlog 对应的数据库。

② 备 iMC 系统 dbman 配置检查。

备 iMC 系统需要勾选“自动恢复模式”。

iMC 服务器地址：127.0.0.1。

数据库地址：集中式部署填写127.0.0.1，分离式部署填写数据库服务器IP地址。

恢复文件路径：主机传输过来的文件存在路径，备iMC系统恢复数据时从该路径读取数据文件。

恢复：勾选表示需要恢复该组件对应的数据。

不允许出现主机未部署而备机部署了某一组件的情况，如图8-507所示。



图8-507　主机未部署而备机部署某一组件

说明：

(a) 保证主、备iMC各组件版本一致。

(b) 根据现场情况建议有选择性的恢复特定的数据库文件。

(10) 日志分析

① 配置生效失败。

如图8-508所示为配置生效操作失败。

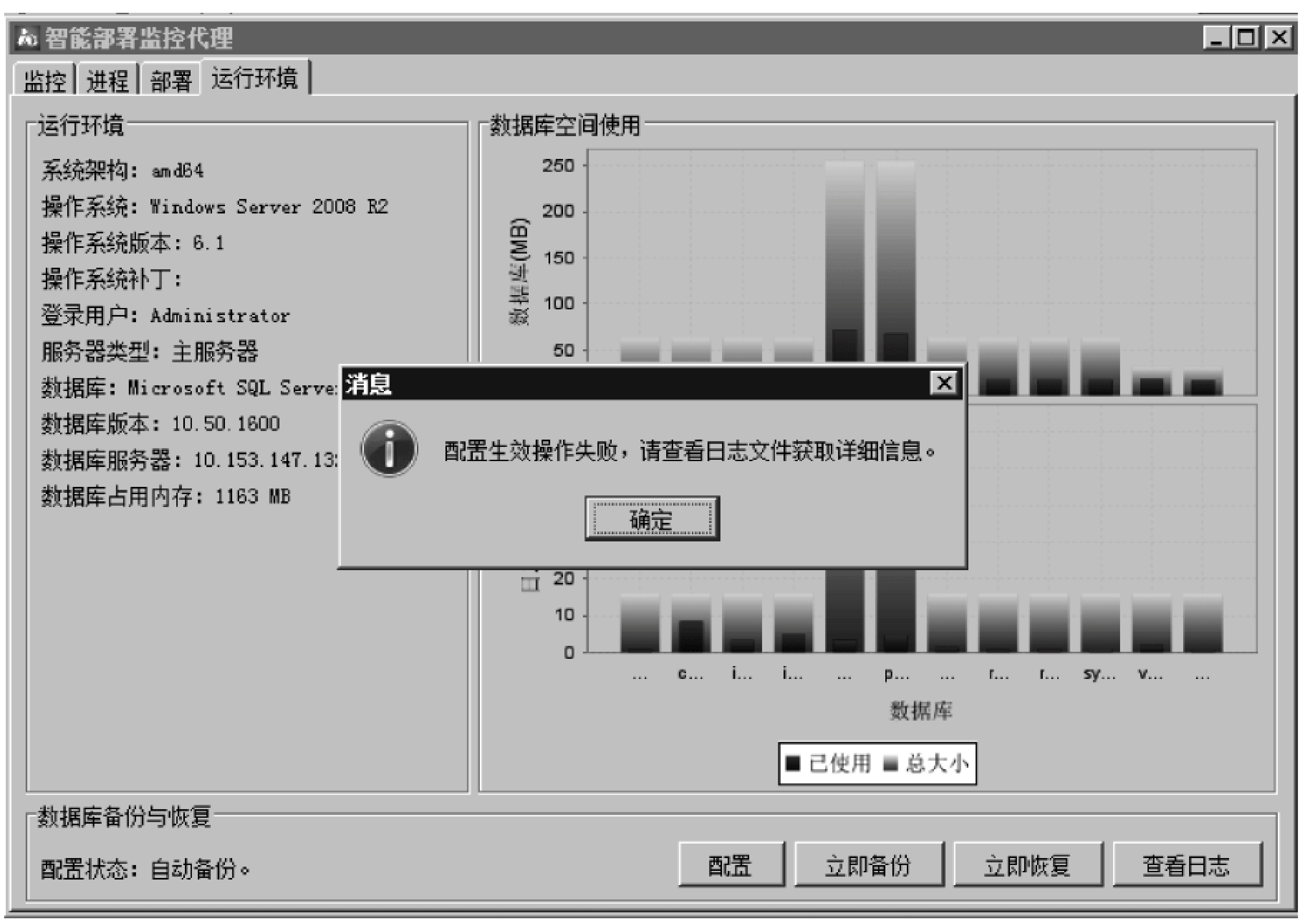


图8-508　配置生效失败

这种情况大部分是数据存放目录不存在导致，dbman_debug.log 日志里一般记录如下。

```
Receive command code: 10020
Input directory invalid: C:\dbmanbaka, code: 1, errCode: -16
errCode = -16.
Fail to create directory
Client close conn
Reload config from file: D:\Program Files\iMC\dbman\bin\..\etc\dbman.conf-errCode = -16.
Client close conn
```

导致该问题的第二种情况如下。

```
Deploy/dma.txt 日志记录如下:
2015-01-06 15:19:32 [ERROR] [SwingWorker-pool-2-thread-10] [com.h3c.imc.deploy.dma.
DBManConfiguration$k::b(5362)] DBMan is backupping
Dbman debuging 日志记录如下:
2015-01-06 15:19:32 [DEBUG] [CDataConnStreamQueueT::deal_msg] Succeed to create
SendBakConfigFileReq thread
2015-01-06 15:19:32 [INFO] [SendBakConfigFileReq] Dbman is backupping
2015-01-06 15:19:32 [DEBUG] [CDataConnStreamQueueT::deal_msg] Client close conn
```

从以上日志看出 dbman 进程挂死，对于这种情况需要将 iMC PLAT 升级至 7.1 E0303H03 及以上版本解决。

说明：

(a) 保证 dbman 配置的路径实际存在。

(b) 其他配置问题也可能导致配置失败。

② 备机没有主机备份的数据。

dbman 要与环境内的所有主机进行通信，包括从机、备机、数据库服务器，在连接不通的情况下是不能进行数据备份的。

dbman 正常通信日志如下。

```
[INFO] [Client::connect_to_server] Starting connect to 127.0.0.1: 2810
[INFO] [Client::connect_to_server] Connection to 127.0.0.1 2810
[DEBUG] [My_Accept_Handler::handle_input] Connection established 127.0.0.1
```

dbman 无法通信日志如下。

```
[INFO] [Client::connect_to_server] Starting connect to 127.0.0.1: 2810
[INFO] [Client::connect_to_server] Connection failed
[ERROR] [Client::send_echo_msg] connect to server fail
```

对于这种情况，一般是备机或数据库服务器防火墙没有关闭，导致主机无法建立到备机 TCP 2810 端口的连接。

说明：建议关闭备机和数据库服务器防火墙。

③ 数据恢复失败。

数据恢复失败问题原因较多，主要有主备 iMC 版本不一致、主备部署组件不一致、丢失 dbman 配置信息、custompage 问题、数据库版本导致。

（a）部署组件不一致时的日志如下。

```
[checkDBFiles] Instance icc_db_imc_icc invalid, there is no information on server
[CDbRestore::RestoreAllDatabase] Fail to check DB file.
[checkDBFile()] File prefix invalid: NICRAC_unba_master, please confirm whether the DB user are same one on main server and standby server.
```

（b）版本不匹配的日志如下。

```
[checkDBFiles] Restore all database failed: Components is not match
[checkDBFiles] Database: config_db. Components:
imc_config_config_db_iMC-PLAT = 7.1.E0303H03
imc_config_config_db_iMC-GAM = 7.1.E0303
imc_config_config_db_iMC-EUPLAT = 7.1.E0303
[checkDBFiles] DbFileConf: config_db_imc_config_db_20141202_154131_full.db
imc_config_config_db_iMC-PLAT = 7.1.E0303
imc_config_config_db_iMC-GAM = 7.1.E0303
```

说明：

ⓐ 保证主、备 iMC 服务器部署组件版本一致。

ⓑ 对于主服务器有而备 iMC 服务器未部署的情况，建议不要在主服务器勾选“上传”。

（c）配置文件丢失时。

分析：dbman 在进行恢复时要检查备份时生成的数据库描述文件 dbman_date_time.conf，找不到该文件时的记录如下。

```
[checkDBFiles] Can not open config file in directory: D:\dbmanrestore
```

此时需要确认对应目录下是否有 dbman_date_time.conf 文件，如果不存在则需要从主机拷贝至备机后再进行恢复。

（d）custompage 问题相关描述如下。

问题日志如下。

```
[CDbRestore::RestoreOneLocalZipFile] Fail to  restore. zip File:D:\beifen\custompage_20140604_102002.zip size compare error localSize=24633248,justfySize=2036115498.
[int Remove()] Fail to remove file D:\beifen\custompage_20140604_102002.zip.
[CDbRestore:: RestoreAllDatabase ( DBFileBoxT& oFileBox, int flag )] Fail to restore strBeforeSQLScript ..\script\iMC-EAD_exec_before.bat 127.0.0.1 ead "iMC5_uameadcams"  "D:\iMC 备份"  "D:\BF"
```

解决方法：删除主备机 iMC\dbman\etc\dbman_addons.conf 中包含 custompage 字眼的行，然后主备都要使配置生效，步骤：依次单击“重启监控代理”→“配置”→“确定”命令。或者升级 PLAT 版本至 7.1 E0303H03 以上。

（e）数据库版本导致时。

问题日志如下。

```
2015-01-14 23:44:38 [ERROR] [CDbRestore::ExecRestoreSql] Exec command fail
2015-01-14 23:44:38 [DEBUG] [CDbRestore::ExecRestoreSql] Exec sql log:消息 3169,级别 16,状态 1,服务器 PLAT,第 1 行该数据库是在运行版本 10.50.1600 的服务器上备份的。该版本与此服务器(运行版本 10.00.5500)不兼容。请在支持该备份的服务器上还原该数据库,或者使用与此服务器兼容的备份。消息 3013,级别 16,状态 1,服务器 PLAT,第 1 行 RESTORE DATABASE 正在异常终止。
2015-01-14 23:44:38 [DEBUG] [Remove] Remove file: D:\Program Files\iMC\dbman\bin\dbop.sql.log
```

从日志可以看出iMC数据是在SQL版本10.50.1600(SQL 2008 R2)版本备份的，需要恢复数据的SQL版本为10.00.5500(SQL 2008 SP3)，由于10.00.5500版本低于10.50.1600导致数据恢复失败；对于iMC dbman备份的数据来说，可以将低版本备份的数据恢复至高版本的SQL(限制条件)，反过来的话由于SQL的限制会导致恢复失败。

解决办法：升级SQL至2008 R2及以上版本。

说明：限制条件如下。

SQL 2000的数据不可以恢复到高版本SQL数据库。

SQL 2005的数据可以恢复到SQL 2008或SQL 2008 R2(包括补丁版本)数据库。

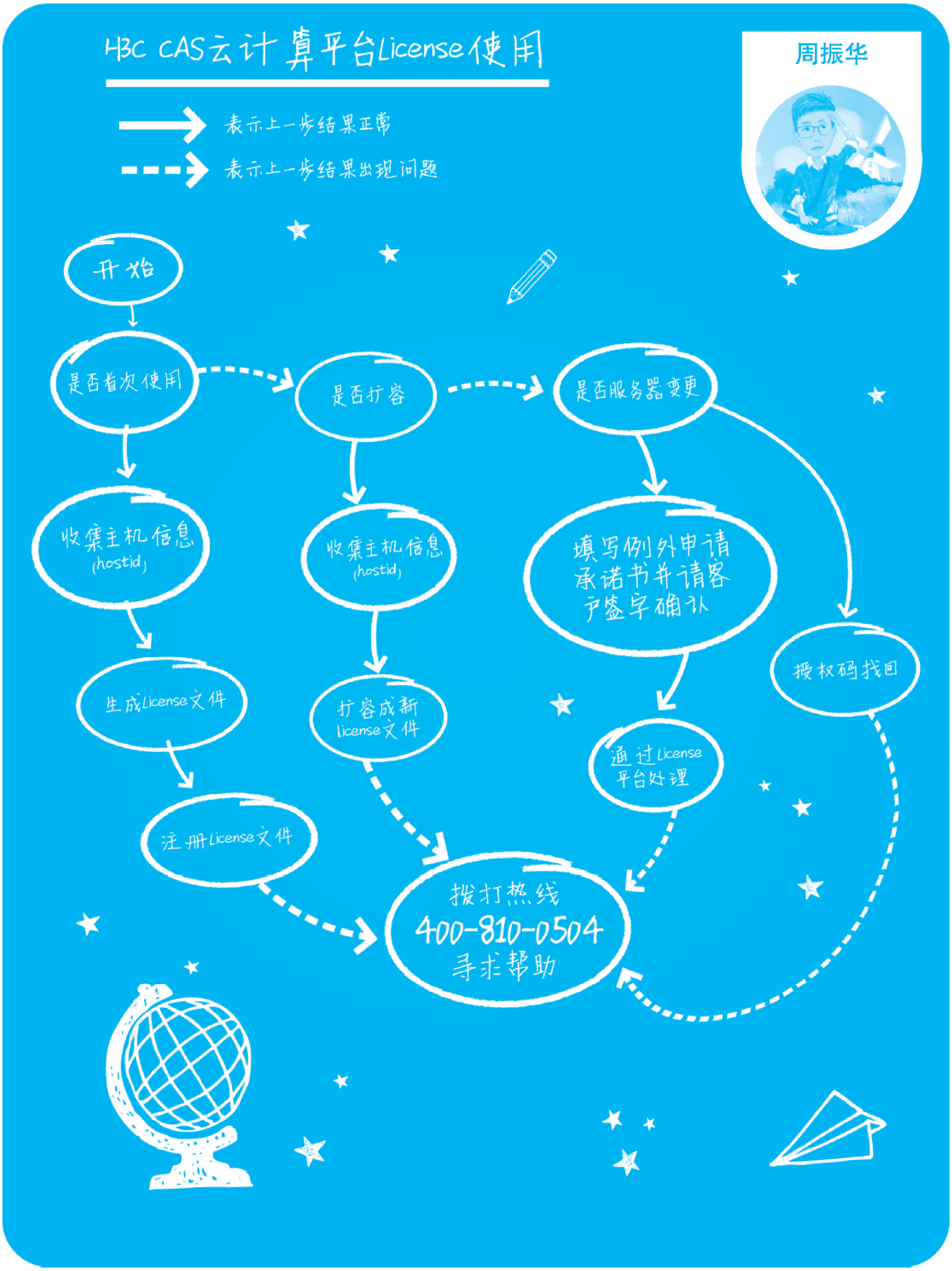
SQL 2008的数据可以恢复到SQL 2008 R2(包括补丁版本)。

SQL 2005的数据不可以恢复到SQL 2012里面。

SQL 2008 R2是否可以恢复到SQL 2014需要确认。

09

云计算产品


H3C CAS云计算平台License使用
周振华
表示上一步结果正常
表示上一步结果出现问题
开始
是否首次使用
是否扩容
是否服务器变更
收集主机信息 (hostid)
收集主机信息 (hostid)
填写例外申请承诺书并请客户签字确认
授权码找回
生成License文件
扩容成新license文件
通过License平台处理
注册License文件
拨打热线 400-810-0504 寻求帮助

1. 开始

H3C CAS 平台的云资源和云服务两大功能依赖于 CVM 组件和 CIC 组件授权，所有的授权码和唯一标识服务器硬件信息的 hostid 进行绑定后生成 License 文件，将 License 文件导入 CAS 平台后，授权才会正式生效。

CVM 组件的授权控制物理 CPU 的个数。比如有 2 台服务器，每台服务器包含 2 路物理 CPU，且每路 CPU 为 6 核，那么我们需要申请的 License 包含 4 个物理 CPU 的 CVM 组件授权。

CVM 组件授权中又分为 CVM 基础包和 CVM 管理包。CVM 基础包为必选，管理包为可选包。如果没有 CVM 基础包，在申请时会提示错误。

CIC 组件的授权控制用户申请虚拟机的数量。比如用户购买了包含 30 个虚拟机的 CIC 组件 License，那么用户可以通过云服务功能申请 30 个虚拟机。

CIC 组件授权中又分为 CIC 基础包和 CIC 管理包。CIC 基础包和管理包都是可选包。

同样 CIC 基础包和 CIC 管理包可以叠加。

在该流程中，有部分操作是相同或类似的，本文档仅对首次出现的流程进行说明。

2. 流程图相关操作说明

(1) 是否首次使用

H3C CAS 软件分为企业版和标准版，因此授权文件也相应分为了企业版和标准版。授权文件不能够混用，即企业版授权文件不能加载到标准版 CAS 系统，同样标准版授权文件不能加载到企业版的 CAS 系统。

说明：首次使用 License 是针对某一个 CAS 的一套授权来讲的，而不是针对某个工程师第一次使用 License。首次使用即表明授权已确定符合客户需求，不涉及服务器变更或授权扩容等情况。

(2) 收集主机信息(hostid)

主机信息是使用服务器硬件信息来唯一标识服务器的，在收集后会形成名为 host.info 的文件。H3C CAS License 需要和 CVM 主机的物理信息进行绑定，以下是两种收集主机信息的方法。

说明：CVM 双机热备组网需要收集两台 CVM 主机信息，详细见(3)。

① License 管理页面获取主机信息。

登录 CAS 系统，选择"系统管理→License 管理"的"正式申请 License"选项卡，如图 9-1 所示。

完成基本信息的填写，并下载"host.info"文件到本地电脑。

② 登录页面获取主机信息。

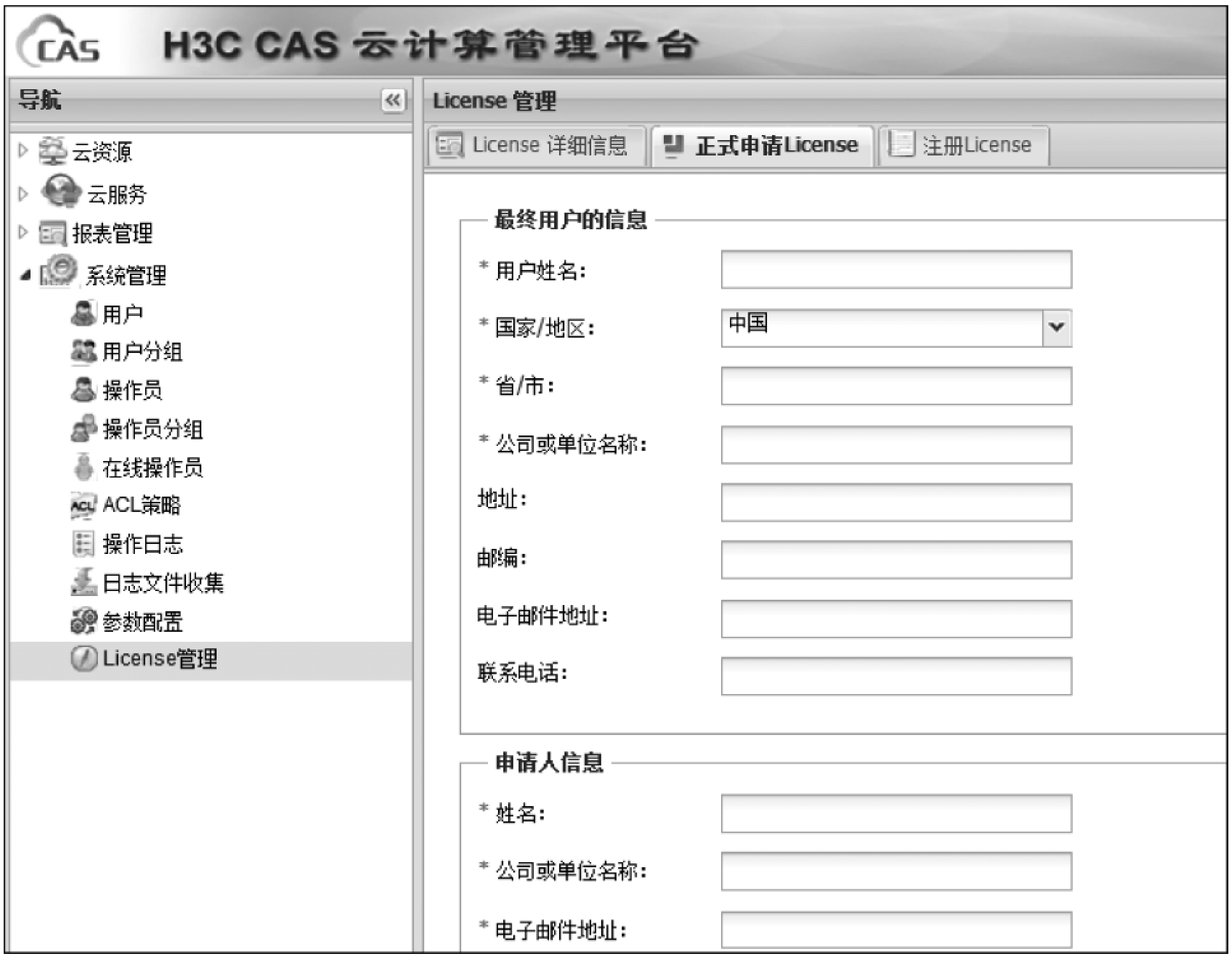


图 9-1 License 管理页面

在浏览器中输入 CAS 系统的 URL 地址(http://ipaddress:port/cas),在登录页面中单击“产品注册”按钮,如图 9-2 所示。



图 9-2 CAS 系统登录页面

在弹出的“产品注册”对话框中的“请输入超级管理(admin)的登录密码”的文本框中输入登录密码，默认密码为 admin。

在“选择您要执行的操作”的下拉列表框中，选择“申请新的 License 或升级现有的 License”。单击“下一步”按钮，如图 9-3 所示。



图 9-3 “产品注册”对话框执行操作

输入“最终用户信息”和“申请人信息”。单击“下一步”按钮，如图 9-4 所示。



图 9-4 “产品注册”对话框信息填写

单击“下载”按钮，将主机信息文件“host.info”下载到本地电脑，如图 9-5 所示。



图 9-5　“产品注册”对话框下载文件

③ 双机热备组网获取主机信息。

CVM 双机热备时需要分别收集两台主机的主机信息，并下载 host.info 文件。

假设当前主机一为 Master，主机二为 Slave。先收集主机一的主机信息，然后收集主机二的主机信息。收集主机二的主机信息前，需要进行主备切换。

主机一信息收集：通过虚拟 IP 登录 CVM 的 Web 收集主机信息，操作方法同(1)(2)。

此时收集的主机一状态为 Master，主机二的状态信息为 Slave。

CVM 双机主备切换：收集完 Master 状态的主机信息后，需要收集 Slave 状态的主机信息。通过 CVM 主备切换，使虚拟 IP 运行在另外一台主机。

命令操作方法：

```
# cvm_resource_start.sh node02
```

主机二信息收集：通过虚拟 IP 登录 CVM 的 Web 收集主机信息，操作方法同(1)(2)。

此时收集的主机一状态为 Slave，主机二的状态信息为 Master。

在首次为 CAS 申请 License 和进行扩容时都需要执行收集主机信息的操作。

(3) 生成 License 文件

生成 License 文件的过程即把授权信息和主机信息进行绑定的过程。首次使用和扩容都需进行此步骤。

在浏览器中输入 H3C 公司网站 URL 地址(www.h3c.com.cn)，选择“服务支持”→“授权业务”命令，如图 9-6 所示。

选择“License 首次激活申请”命令，显示“License 首次激活”页面。

说明：*在扩容时，选择“License 激活管理”→“License 扩容激活申请”命令，其他操作类似。*



图 9-6 H3C 公司网站授权业务

在"产品分类"下拉列表框中选择"云计算_H3C CAS 云计算管理平台"命令，如图 9-7 所示。



图 9-7 H3C 公司网站 License 首次激活

"授权信息"中选择方式二添加 CVM 和 CIC 的授权码信息(不要添加 CAS 软件授权码)。

"设备信息"中的"请选择双机备份类型"栏根据现场实际情况选择，如果 CVM 为单机，则单击"无"单选按钮；如果 CVM 为双机，则单击"双机热备"单选按钮。以 CVM 单机为例，单击"无"单选按钮。在"设备信息"栏单击"上传"按钮上传"host.info"文件，如图 9-8 所示。

在"用户信息"中输入必填信息后单击"获取激活码(文件)"，将激活文件下载本地电脑，如图 9-9 所示。

(4) 注册 License 文件

以下是两种注册 License 的方法。

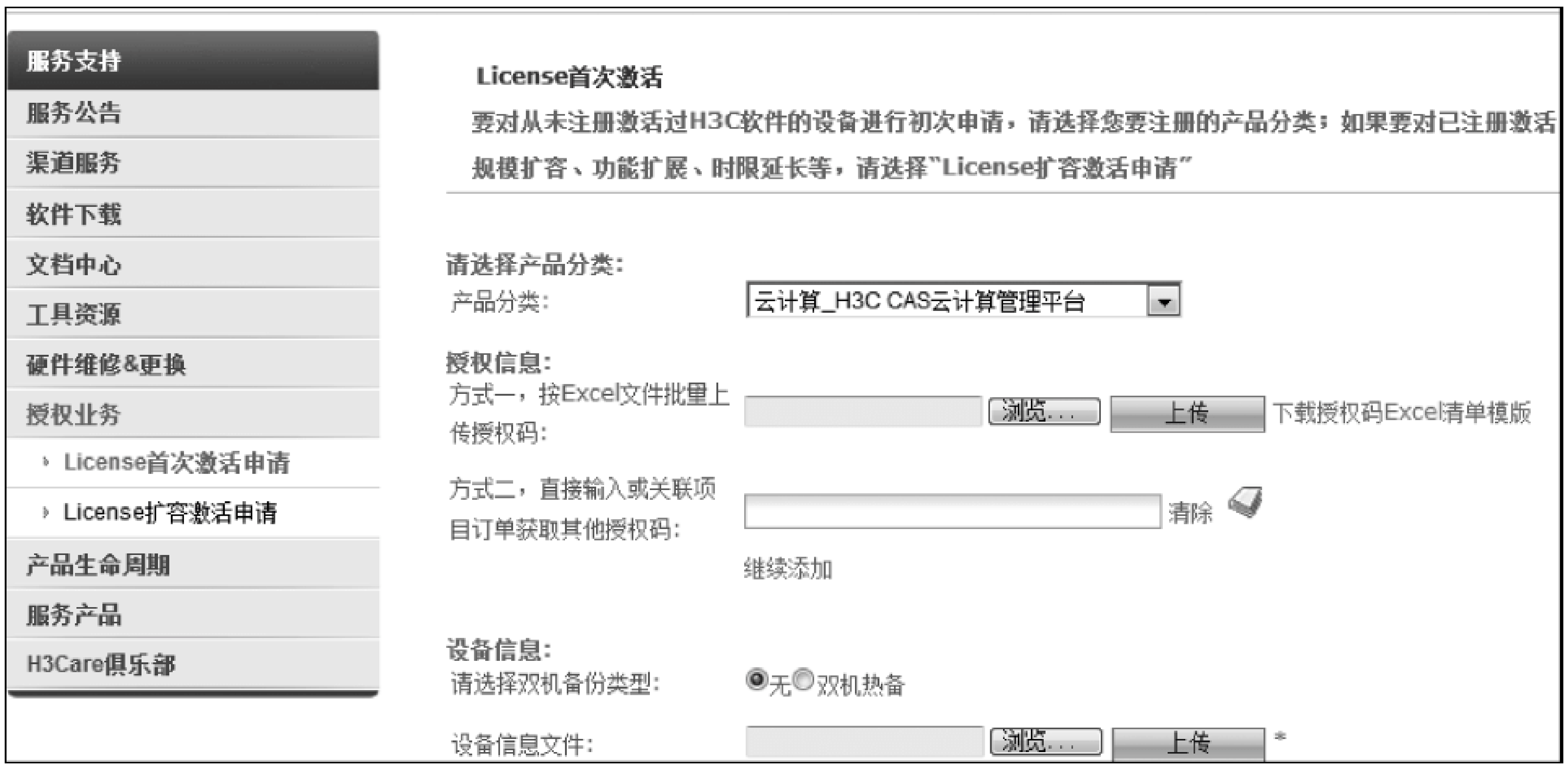


图 9-8　H3C 公司网站 License 首次激活信息填写

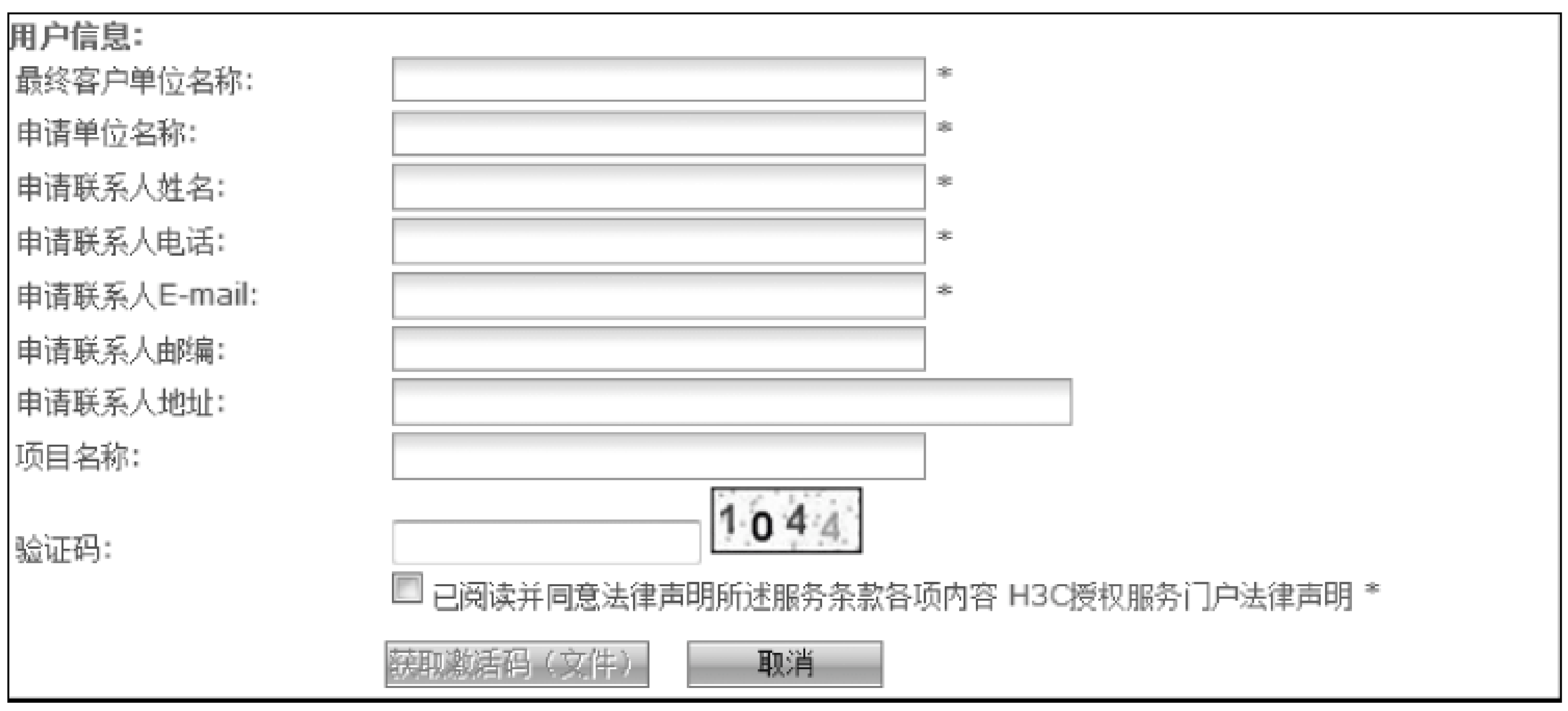


图 9-9　激活文件

说明： CVM 双机热备组网需要注册到两台 CVM 主机，详细见(3)。

① License 管理页面注册。

选择"系统管理"→"License 管理"的"注册 License"选项卡，单击"浏览"按钮选择 License 激活文件，然后单击"上传"按钮进行注册，如图 9-10 所示。

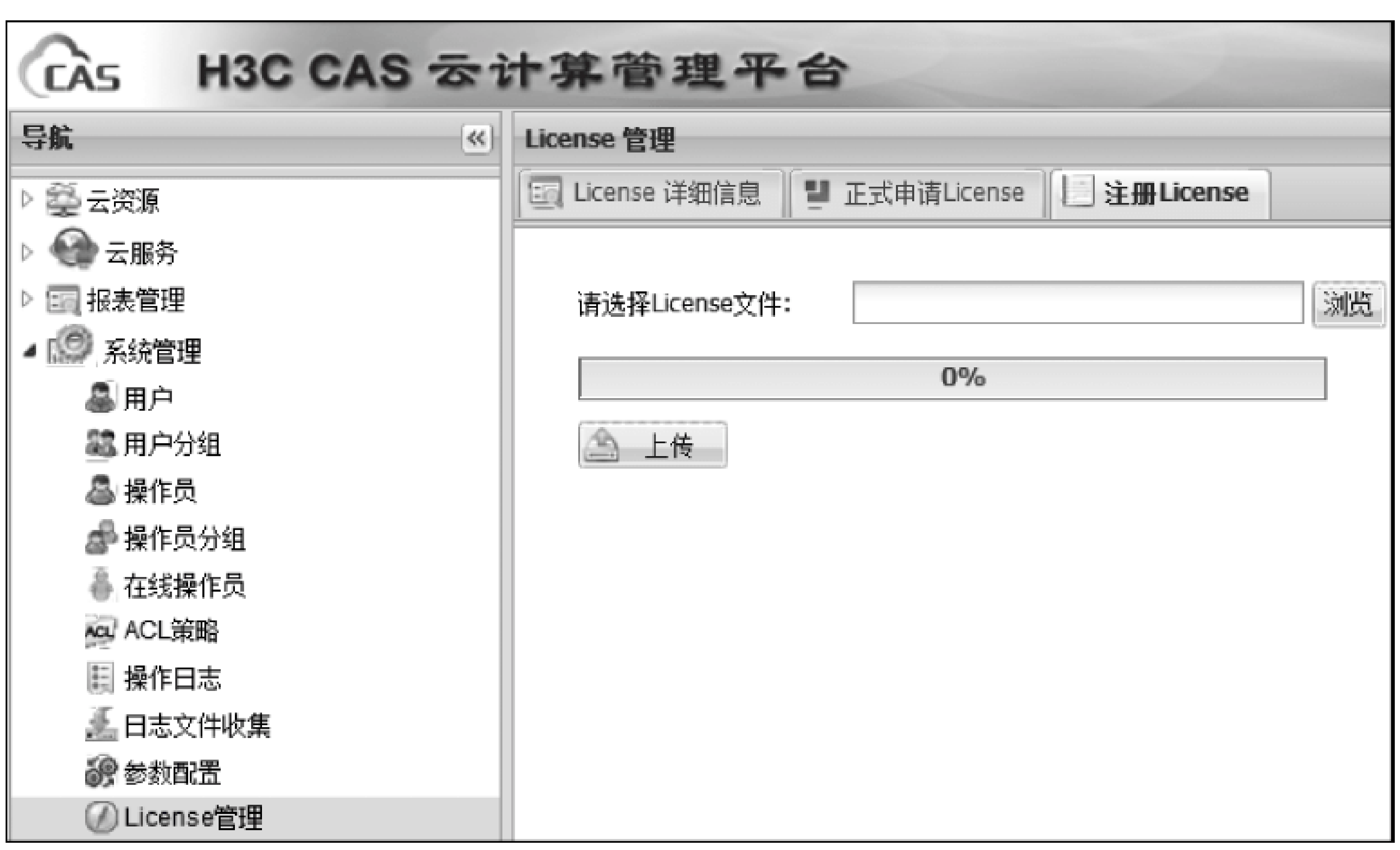


图 9-10　License 注册

② 登录页面注册。

在如图 9-11 所示的“选择您要执行的操作”的下拉列表框中选择“使用 License 文件对产品进行注册”命令。



图 9-11 使用 License 文件对产品进行注册

在“请选择 License 文件”栏单击“浏览”按钮选择 License 激活文件。

然后单击“上传”按钮进行注册，如图 9-12 所示。

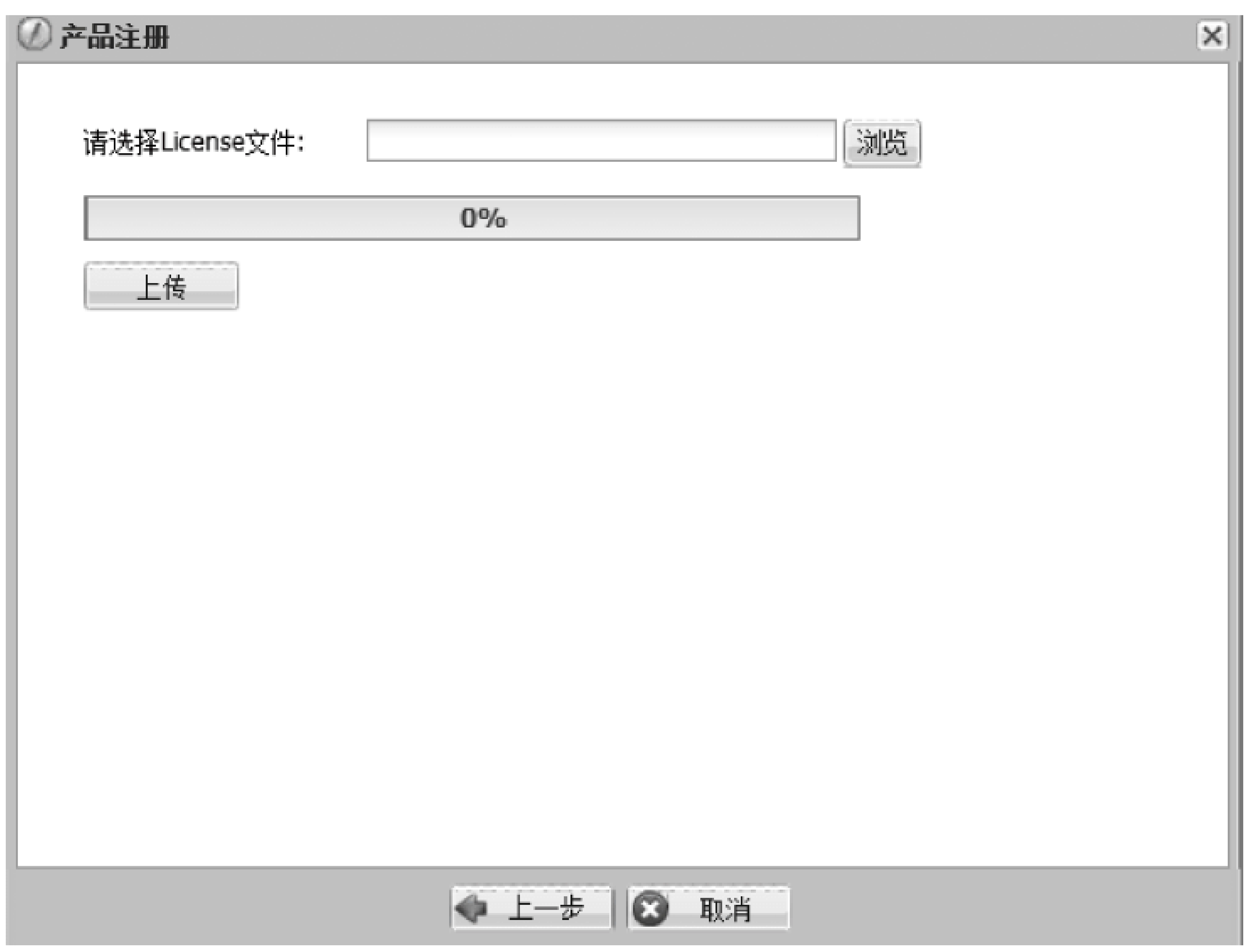


图 9-12 登录页面注册

③ CVM 双机组网注册 License。

假设当前主机一为 Master，主机二为 Slave。先对主机一注册 License，然后对主机二注册 License。主机二注册 License 前，需要进行主备切换。

主机一注册 License：注册方法同(1)(2)。

CVM 双机主板切换：完成 Master 状态的主机 License 注册后，需要对 Slave 状态的主机注册 License。通过 CVM 主备切换，使虚拟 IP 运行在另外一台主机。

命令操作方法如下。

```
# cvm_resource_start.sh node02
```

主机二注册 License：注册 License 文件方法同(1)(2)。

④ License 注册完成后显示。

License 注册完成后，在“系统管理→License 管理”的“License 详细管理”选项卡中显示 License 信息。

在“License 详细信息”中包含了四个部分：CVM 组件、CIC 组件、版本和 License 有效期，如图 9-13 所示。



图 9-13 License 详细信息

(5) 是否扩容

正式 License 扩容申请和正式 License 首次申请操作方法基本相同。在“设备信息”中要上传“历史激活文件”。

正式 License 扩容时，不依赖于 CVM 基础包，可以直接输入 CVM 管理包的授权码。

扩容后生成的激活文件会叠加原 License 信息。比如原 License 中包含了 4 个物理 CPU 和 30 个虚拟机，扩容时输入的授权码包含 8 个物理 CPU 的 CVM 管理包和 50 个虚拟机的 CIC 管理包，那么扩容后生成的激活文件包含 12 个物理 CPU 和 80 个虚拟机。

(6) 扩容成新 license 文件

扩容激活有 2 种方法，如图 9-14 所示。

① 上传最新的历史激活文件：最新的历史激活文件是指我们上次通过 License 平台获取到的最新的激活文件，可以通过当时留下的注册邮箱查找。

② 上传服务器主机信息：收集目前运行主机的 host.id 信息。

通过上述 2 种方式都可以进行扩容激活。历史激活文件包含了历史的授权码信息和服务器主机信息。最新的服务器主机信息也是包含了历史授权码和主机信息，最后的效果一致。



图 9-14　扩容激活的方法

（7）是否变更服务器

H3C CAS License 加载在 CVM 主机。完成 License 加载后，发生 CVM 主机故障等情况时，需要更换 CVM 主机。这时需要在新的 CVM 主机上加载 License 文件。

新 License 文件获得需要在 License 平台中选择“设备更换授权变更管理”→“设备更换授权变更申请”命令，如图 9-15 所示，进行操作，在操作前应准备好客户承诺书以及新老服务器的 host. info 文件。



图 9-15　设备更换授权变更申请

说明：新老服务器的 host. info 获取方法详见“检查主机信息(hostid)”步骤。

（8）填写例外申请承诺书并请客户签字确认

客户承诺书可在 H3C 内部网站 DMP 下载。

在申请 License 前需要客户填写《H3C CAS 云计算管理平台 License 例外申请及承诺书》，如图 9-16 所示并由客户签字盖章。

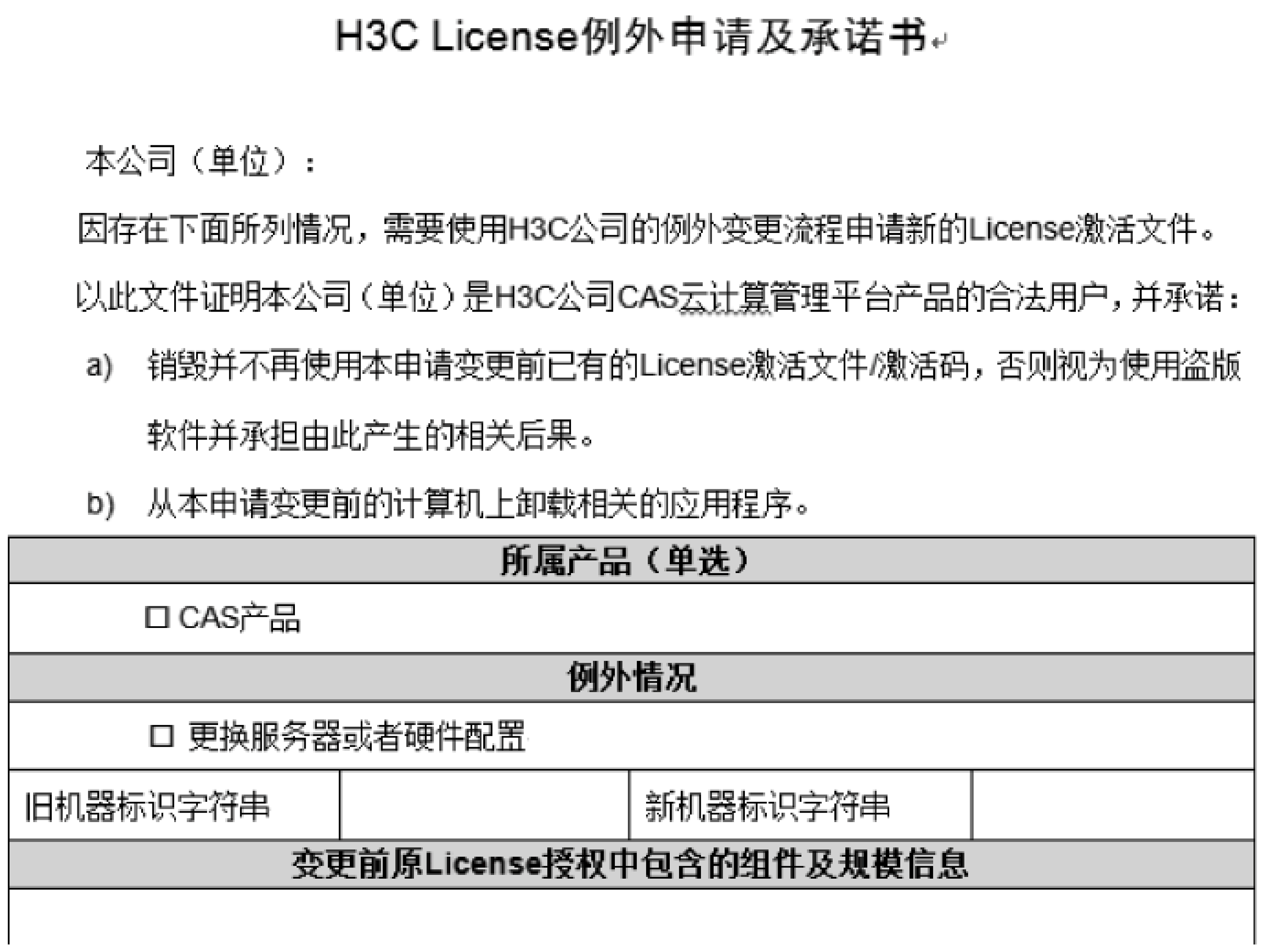
将该文件扫描成电子件，后续申请时使用该电子件。

《H3C CAS 云计算管理平台 License 例外申请及承诺书. doc》获取方法如下。

公司 DMP 网站，URL 地址为“http://dmp. h3c. com”，存放路径为“技术支持中心→01-IP 网络产品→60-2013 产品→02-工程、开局资料”。

（9）通过 License 平台处理

上传“原服务器关联的激活码（文件）”或者“原服务器关联的授权码”，再根据提示进行下



H3C License例外申请及承诺书

本公司（单位）：

因存在下面所列情况，需要使用H3C公司的例外变更流程申请新的License激活文件。

以此文件证明本公司（单位）是H3C公司CAS云计算管理平台产品的合法用户，并承诺：

a) 销毁并不再使用本申请变更前已有的License激活文件/激活码，否则视为使用盗版软件并承担由此产生的相关后果。

b) 从本申请变更前的计算机上卸载相关的应用程序。

所属产品（单选）			
☐ CAS产品			
例外情况			
☐ 更换服务器或者硬件配置			
旧机器标识字符串		新机器标识字符串	
变更前原License授权中包含的组件及规模信息			

图 9-16　H3C License 例外申请及承诺书

一步操作，如图 9-17 所示。

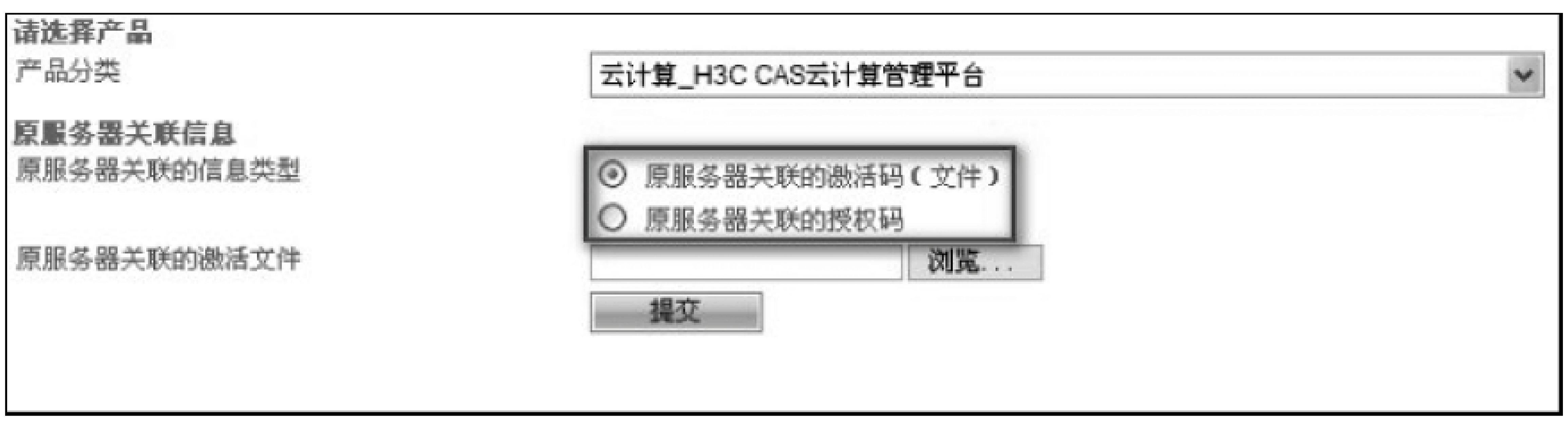


图 9-17　通过 License 平台处理

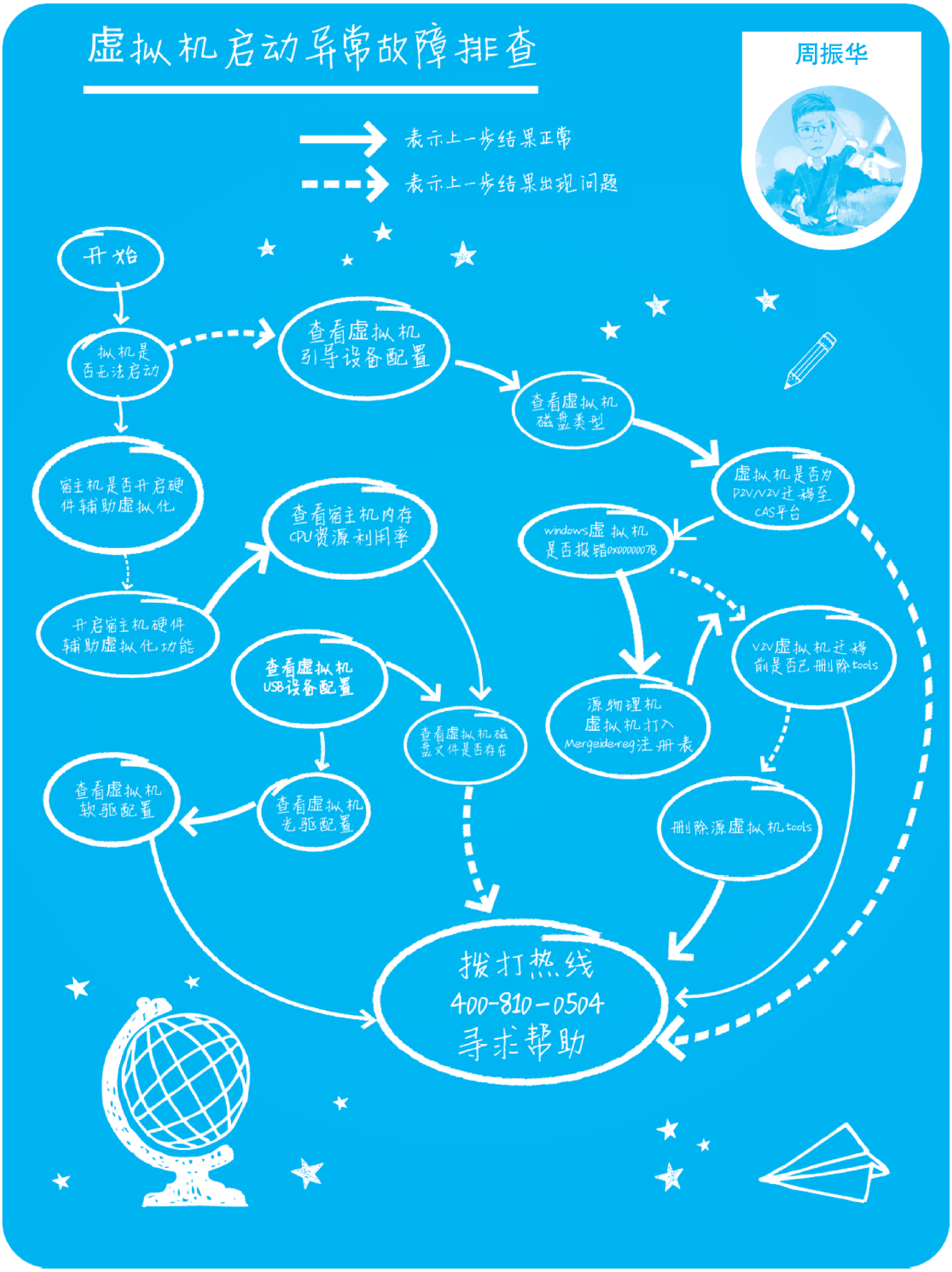
（10）授权码找回

授权码若丢失了可以通过 LMP 平台找回授权码，如图 9-18 所示。



图 9-18　通过 LMP 平台找回授权码

可以通过订单号或者软件条码进行找回。


虚拟机启动异常故障排查
周振华
表示上一步结果正常
表示上一步结果出现问题
开始
拟机是否无法启动
查看虚拟机引导设备配置
查看虚拟机磁盘类型
虚拟机是否为P2V/V2V迁移至CAS平台
宿主机是否开启硬件辅助虚拟化
开启宿主机硬件辅助虚拟化功能
查看宿主机内存CPU资源利用率
windows虚拟机是否报错0x0000007B
源物理机虚拟机打入Mergeide.reg注册表
V2V虚拟机迁移前是否已删除tools
删除源虚拟机tools
查看虚拟机USB设备配置
查看虚拟机磁盘文件是否存在
查看虚拟机光驱配置
查看虚拟机软驱配置
拨打热线
400-810-0504
寻求帮助

1. 开始

虚拟机是指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。虚拟机启动异常分为两种情况：虚拟机无法启动和虚拟机启动后无法进入操作系统。

对于虚拟机无法启动的情况：由于虚拟机依附于宿主机而存在，因此问题定位思路是，先检查宿主机配置和状态，再检查虚拟机自身配置。

对于虚拟机启动后无法进入操作系统情况：需要查看虚拟机引导设备和磁盘类型，对于P2V/V2V迁移至CAS平台的虚拟机，需要确认的是在迁移之前打入mergeide.reg注册表，并且V2V迁移之前需要卸载tools。

2. 流程图相关操作说明

（1）虚拟机是否无法启动

如果虚拟机无法启动，在任务栏会有“启动失败”的报错，如图9-19所示。

如果虚拟机启动成功，在任务栏会有“启动成功”的提示，如图9-20所示。

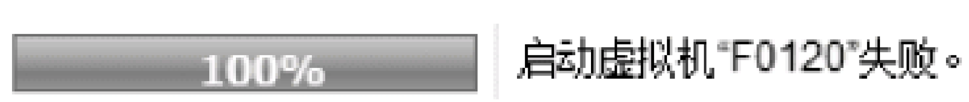


图 9-19 虚拟机启动失败报错

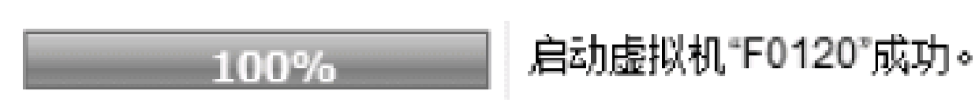


图 9-20 虚拟机启动成功提示

（2）宿主机是否开启硬件辅助虚拟化

查看宿主机是否开启硬件辅助虚拟化功能。

命令：*lsmod | grep kvm*

例如：通过命令查看，可以确认宿主机加载了KVM模块，表示硬件辅助虚拟化功能已经开启，如果输入命令没有任何输出，说明宿主机未开启硬件辅助虚拟化。

```
root@HZ-CAS01-CVK01:~# lsmod | grep kvm
kvm_intel              123137   21
kvm                    336971   1 kvm_intel
```

（3）开启宿主机硬件辅助虚拟化功能

宿主机启动时在硬件自检界面按F9键进入BIOS，如图9-21所示。

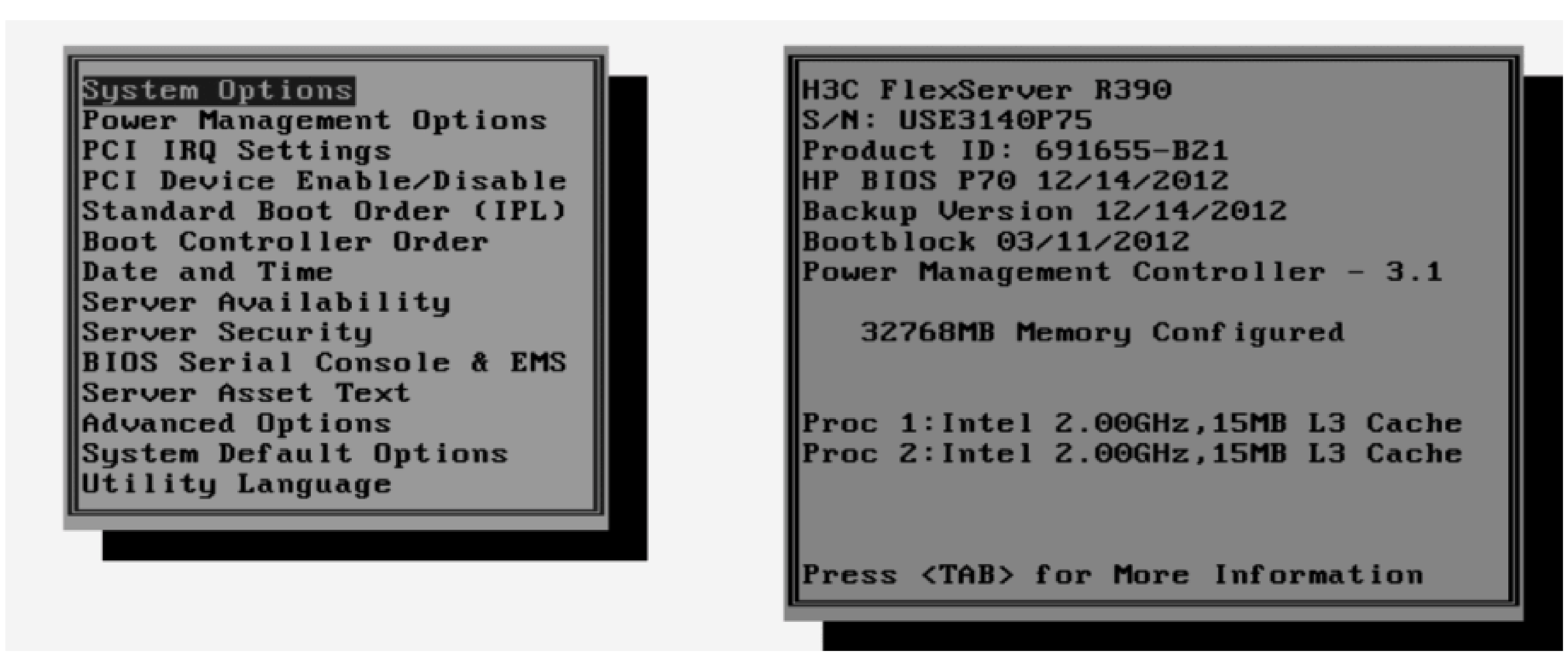


图 9-21 进入 BIOS

选择 System Options 命令，在弹出的对话框中选择 Processor Options 命令，如图 9-22 所示。



图 9-22 进入 Processor Options

选择 Intel(R) Virtualization Technology 命令，开启硬件辅助虚拟化功能，如图 9-23 所示。



图 9-23 开启硬件辅助虚拟化功能

(4) 查看宿主机内存、CPU 资源利用率

CAS 管理界面单击主机，在“概要”选项卡右上角统计栏查看主机实时内存、CPU 利用率统计。如果宿主机剩余内存、CPU 资源小于所需启动的虚拟机内存、CPU 配置，则虚拟机会因资源不足而无法正常启动，关闭或者迁移暂时不需要使用的虚拟机，如图 9-24 所示。

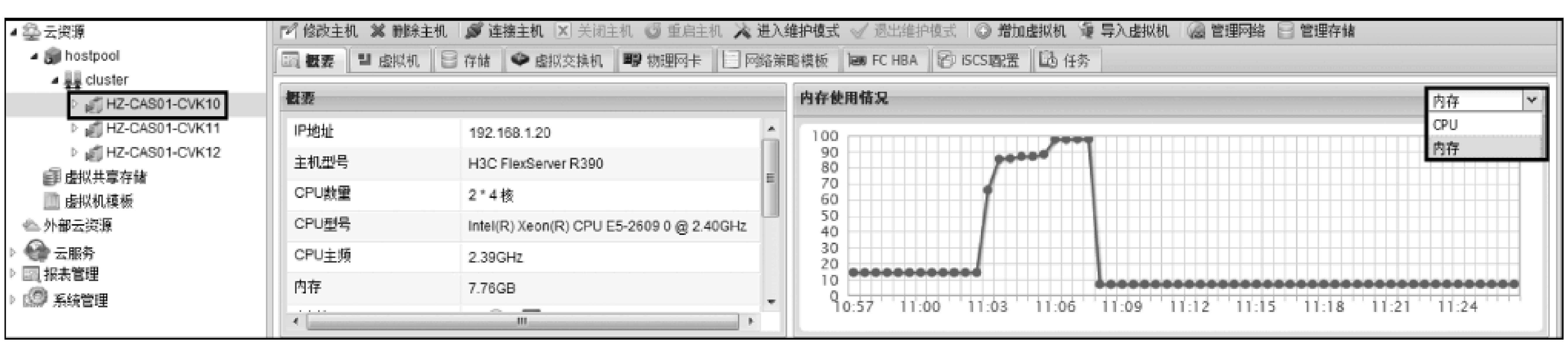


图 9-24 查看宿主机内存、CPU 资源利用率

(5) 查看虚拟机磁盘文件是否存在

单机虚拟机，在“概要”选项卡的“存储信息”栏中，查看虚拟机的虚拟磁盘文件以及基础镜像文件的名称和路径，如图 9-25 所示。

存储信息

	设备名称	总线类型	存储卷名称	容量	类型	基础镜像文件
磁盘	hda	ide	/vms/images/win2008-vCenter-clone	39.06GB	文件	/vms/images/win2008-vCenter_base_0
光驱	hdc	ide		0.00MB	文件	

图 9-25 查看虚拟机磁盘是否存在

确认虚拟机的虚拟磁盘文件以及基础镜像文件的存在。

命令：*ls -l*

例如：进入虚拟机虚拟磁盘文件所在目录，通过命令查看，可以确认虚拟机的虚拟磁盘文件以及基础镜像文件存在，如图 9-26 所示。

```
root@HZ-CAS01-CVK02:/vms/images# ls -l
total 85581940
drwxr-xr-x   3  root root         4096  Dec 10 22:31  ./
drwxr-xr-x  10  root root         4096  Dec 13 01:08  ../
-rw-------   1  root root  12861833216  Dec 10 22:05  vCenter-chunjing
-rw-r--r--   1  root root  15929966592  Dec 13 23:13  win2008-vCenter
-rw-r--r--   1  root root  14413725696  Dec  1 01:53  win2008-vCenter_base_0
-rw-------   1  root root   1382023168  Dec 10 20:22  win2008-vCenter-clone
-rw-------   1  root root  12889096192  Dec 12 00:27  win2008-vCenter-S1010V
-rw-------   1  root root   7862222848  Dec  9 23:10  win2008-vCenter-vs-clone
```

图 9-26 虚拟机虚拟磁盘文件所在目录

(6) 查看虚拟机 USB 设备配置

确认虚拟机配置的 USB 设备已经插入对应的宿主机 USB 插槽，如图 9-27 所示。如果宿主机没有插入 USB 设备，请删除虚拟机上的 USB 设备。

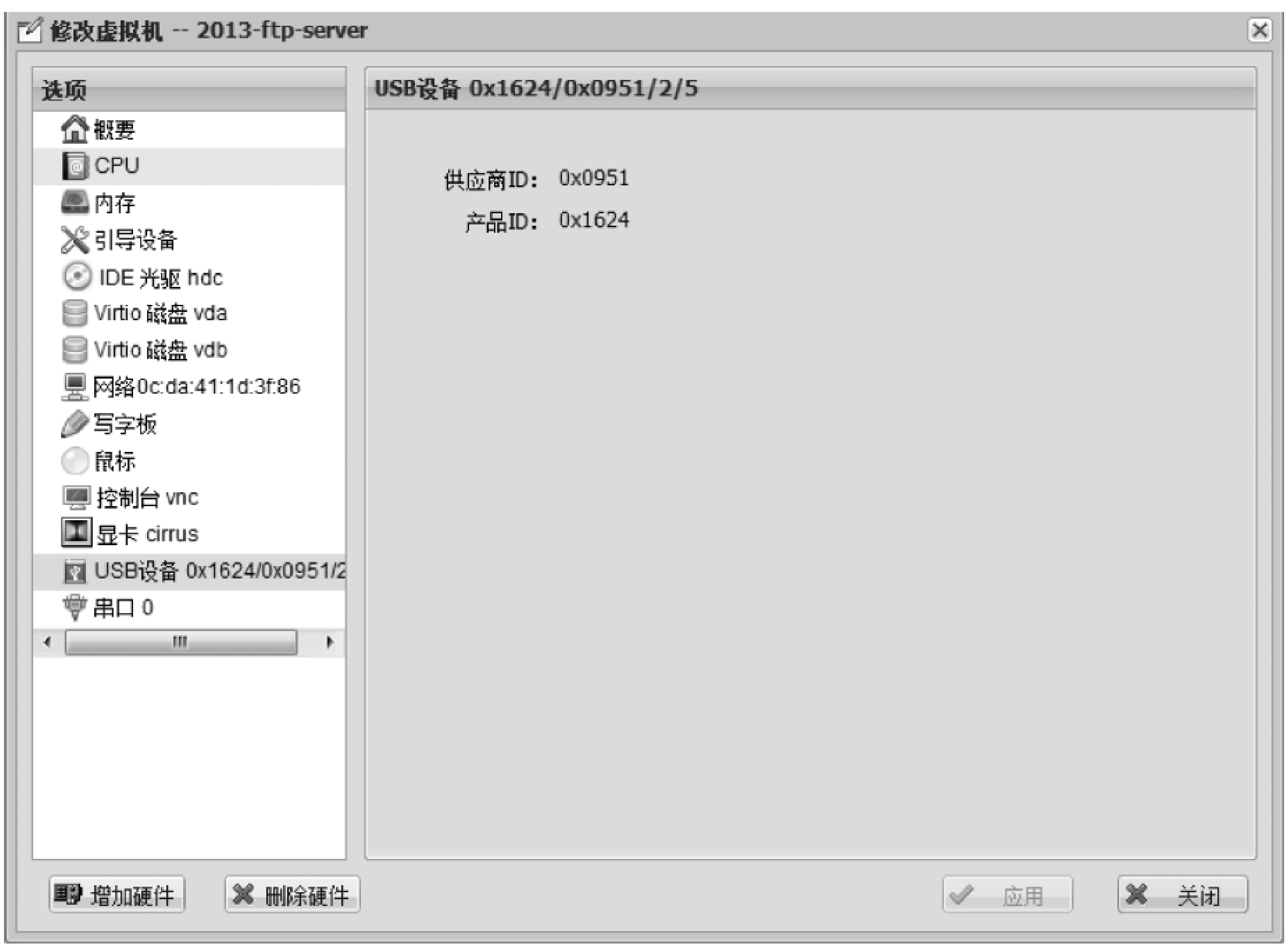


图 9-27 虚拟机 USB 设备配置

（7）查看虚拟机光驱配置

如果光驱源路径是→“dev”→“cdrom”，表示虚拟机使用所在宿主机光驱，需要确保宿主机有光驱，如图 9-28 所示。



图 9-28　虚拟机光驱配置

（8）查看虚拟机软驱配置

软驱中加载的文件必须为软驱文件，如图 9-29 所示，后缀名为. vfd，如果挂载其他格式的文件则虚拟机无法启动。



图 9-29　虚拟机软驱配置

（9）查看虚拟机引导设备配置

如果虚拟机有多个磁盘，需要确保安装系统的磁盘引导优先级最高。在“修改虚拟机”对话框的“选项”栏选择“引导设备”命令，然后在右边“引导设备”复选框勾选需要修改优先级的设备，单击“⇧”按钮，并应用配置，如图 9-30 所示。修改引导设备需要虚拟机重启生效。



图 9-30 修改磁盘引导优先级

（10）查看虚拟机磁盘类型

如果虚拟机磁盘为 SCSI 磁盘或者 virtio 磁盘，如图 9-31 所示，需要确保操作系统已经安装对应的驱动，否则系统无法引导。



图 9-31 虚拟机磁盘类型

(11) 虚拟机是否为 P2V/V2V 迁移至 CAS 平台

确认虚拟机是 P2V/V2V 迁移至 CAS 平台的还是在 CAS 平台创建的。

(12) Windows 虚拟机是否报错 0x0000007B

P2V/V2V 迁移后的 Windows 虚拟机启动,查看在进入操作系统过程中是否有报错 0x0000007B,详细报错信息如图 9-32 所示。

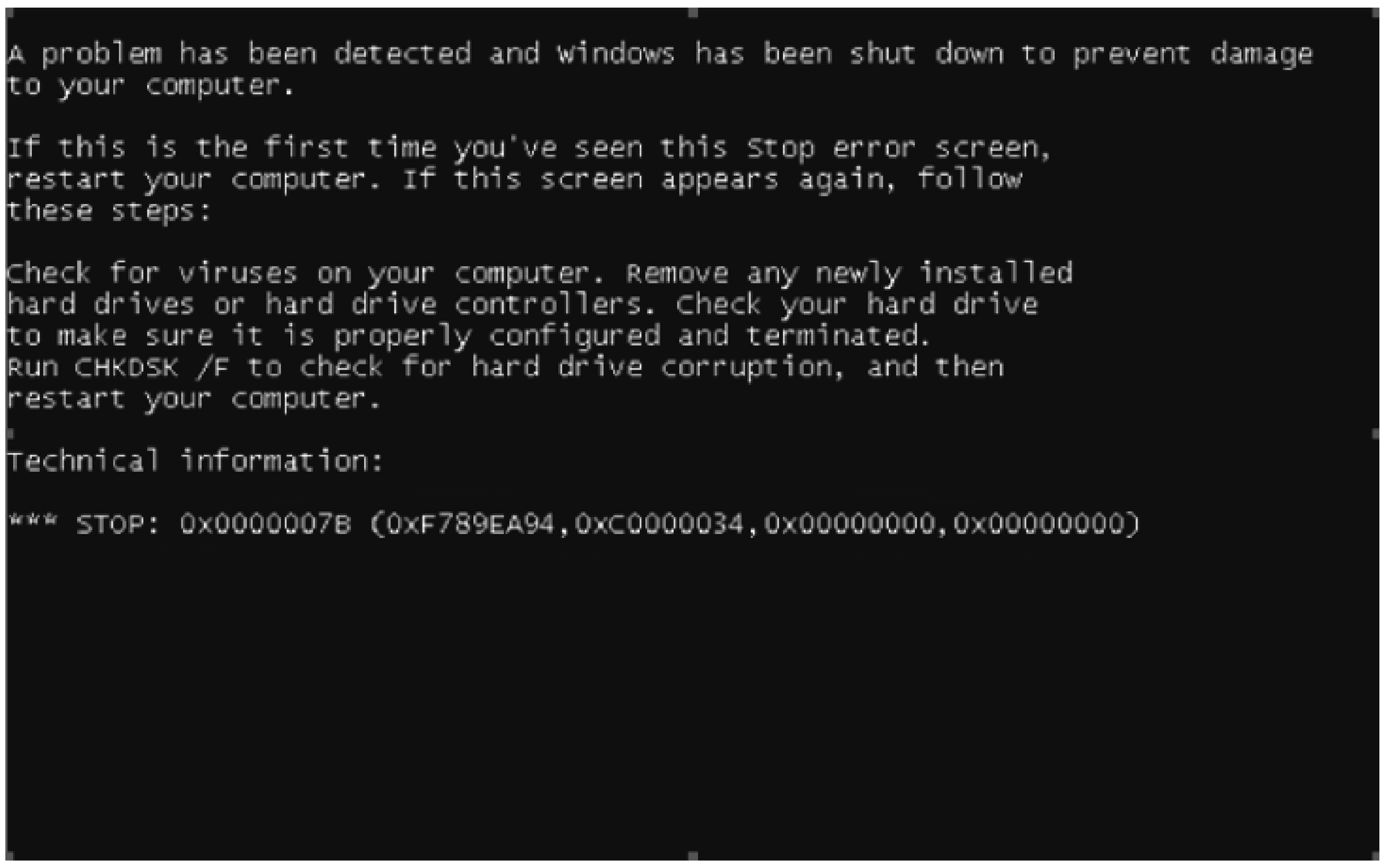


图 9-32 报错信息

(13) 源物理机/虚拟机打入 Mergeide.reg 注册表

在源物理机/虚拟机中运行 Mergeide.reg 注册表,并保证系统分区的"Windows"→"system32"→"drivers"→目录下存在 atapi.sys、intelide.sys、pciide.sys 和 pciidex.sys 四个文件。

(14) V2V 虚拟机迁移前是否已删除 tools

确认 V2V 虚拟机在迁移之前是否已经删除相应的 tools。

(15) 删除源虚拟机 tools

虚拟机的 tools 与平台关联性较强,如果迁移至其他虚拟化平台则无法正常运行,会导致各类问题,因此在 V2V 迁移之前,需要删除虚拟化平台的 tools。


零存储集群添加
节点异常故障排查
陈明槐
表示上一步结果正常
表示上一步结果出现问题
开始
检查各配置
文件存在情况
检查各类
配置文件内容
检查数据
磁盘挂载点
删除数据
磁盘内数据
检查UMP
界面配置
检查虚拟共
享存储配置
拨打热线
400-810-0504
寻求帮助

1. 开始

零存储集群添加节点需要检查配置文件、磁盘数据、TCP 端口等多项内容，涉及的内容较多且较复杂。故障大概可以分为以下五大类。

① 各类配置文件有多余或缺失。

② 配置文件内容错误。

③ 数据磁盘配置问题。

④ UMP 界面配置错误。

⑤ 3260 端口被占用。

2. 流程图相关操作说明

(1) 检查各配置文件存在情况

在"/opt/mds/etc"目录下使用 ll 命令如图 9-33 所示。

```
root@HZ-CAS01-CVK01:/opt/mds/etc# ll
total 28
drwxr-xr-x  3  root root  4096  Aug   3  17:51  ./
drwxr-xr-x  7  root root  4096  Aug   3  17:51  ../
-rw-r--r--  1  root root    53  Sep  27   2013  cgroup.conf
-rw-r--r--  1  root root    22  Jul  17   2013  cluster.conf
-rw-r--r--  1  root root    28  May  13  18:19  hosts.conf
-rw-r--r--  1  root root   426  Aug   3  17:51  lich.conf
drwxr-xr-x  3  root root  4096  Aug   3  17:52  ump/
```

图 9-33 各配置文件存在情况

默认安装完 CAS 以后，会存在 hosts.conf 文件、lich.conf 文件和 cgroup.conf 文件，cluster.conf 文件不会存在。

① 如果有如图 9-34 所示报错，可以判定为存在 cluster 文件。



图 9-34 存在 cluster 文件报错

通过使用 rm 命令手工删除 cluster. conf 文件。

```
root@HZ-CAS01-CVK01:/opt/mds/etc# rm cluster.conf
```

② 如果有如图 9-35 所示报错,可以判定为缺少 hosts. conf 文件。

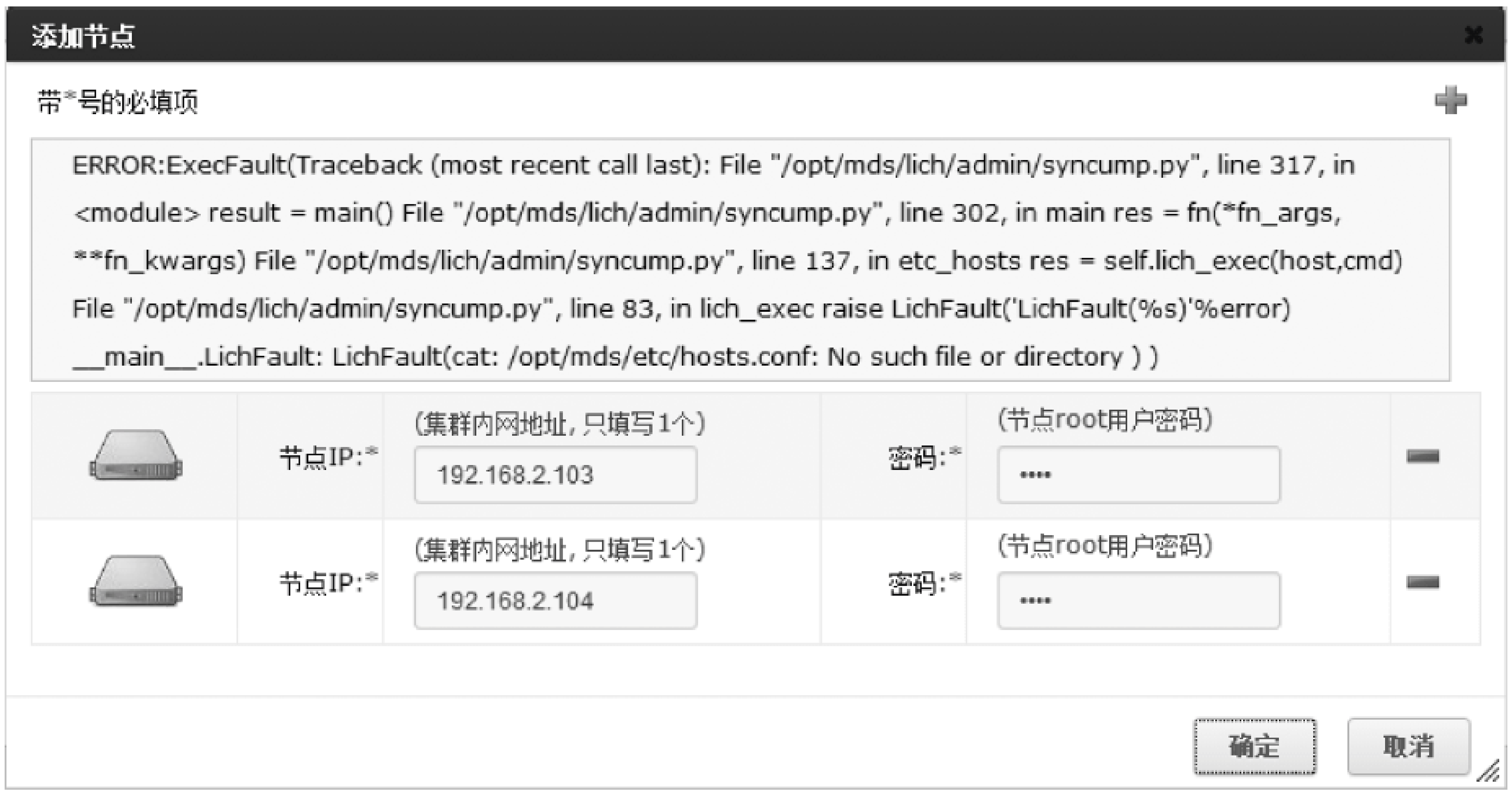


图 9-35　缺少 hosts. conf 文件报错

使用 touch 命令添加一个空白 hosts. conf 文件,文件中不需要输入任何内容。

```
root@HZ-CAS01-CVK01:/opt/mds/etc# touch hosts.conf
```

③ 如果有如图 9-36 所示报错,可以判定为缺少 lich. conf 文件。



图 9-36　缺少 lich. conf 文件报错

通过 scp 命令从其他主机拷贝一个文件至此主机。

```
root@HZ-CAS01-CVK02:/opt/mds/etc# scp lich.conf 10.88.8.39:/opt/mds/etc/lich.conf
Warning: Permanently added '10.88.8.39' (ECDSA) to the list of known hosts.
lich.conf
```

(2) 检查各类配置文件内容

集群添加节点时系统会对各类配置文件的内容进行检查,如果内容不符合要求则节点无法添加到集群中。host.conf 文件记录了节点主机名和存储内网 IP 的映射,节点未加入集群时此文件必须为空;lich.conf 配置是零存储的主要配置文件,记录了集群名称、target 前缀、存储内网网段信息等信息,除了存储内网网段信息必须在后台配置外,其他信息都可以通过 UMP 界面配置并同步至后台配置文件,networks 字段必须配置 24~30 位掩码的网段。

① 如果有如图 9-37 所示报错,可以判定为 hosts.conf 文件中有内容。



图 9-37 hosts.conf 文件中有内容报错

通过 vim 编辑 hosts.conf 文件,删除文件中的内容

```
root@HZ-CAS01-CVK01:/opt/mds/etc# vim hosts.conf
```

② 如果有如图 9-38 所示报错,可以判定存储内网掩码超出范围。



图 9-38 存储内网掩码超出范围报错

登录 CAS 平台,单击需要修改的节点,选择“虚拟交换机”对话框,然后修改存储内网 vswitch,保证掩码在指定范围内,如图 9-39 所示。



图 9-39 “修改虚拟交换机”对话框

登录 CAS 后台，使用 vim 修改 lich.conf 配置文件，将 networks 段的存储内网网段掩码修改为相应位数。

```
root@HZ-CAS01-CVK01:/opt/mds/etc# vim lich.conf
globals {
#clustername mds;
        home /opt/mds;
        #arbitor 10.88.8.1;
        nohosts on;
        networks {
              10.0.132.0/16;
        }
}
iscsi {
        iqn iqn.2001-04-123.com.h3c;
}
```

（3）检查数据磁盘挂载点

对于零存储来说，每个节点上的数据磁盘数量和挂载点数量必须一致，且挂载点必须从 0 开始依次编号，如果挂载点数量大于数据磁盘数量，则无法将节点添加进集群中。在“/opt/mds/disk”目录下通过 ll 命令查看存在的挂载点数量。

```
root@HZ-CAS01-CVK01:/opt/mds/disk# ll
total 28
drwxr-xr-x 7 root root 4096 Oct 14 13:47 ./
drwxr-xr-x 7 root root 4096 Aug  3 17:51 ../
drwxr-xr-x 2 root root 4096 Aug  3 17:51 0/
drwxr-xr-x 2 root root 4096 Oct 14 13:47 1/
drwxr-xr-x 2 root root 4096 Oct 14 13:47 2/
drwxr-xr-x 2 root root 4096 Oct 14 13:47 3/
drwxr-xr-x 2 root root 4096 Oct 14 13:47 4/
```

如果存在如图 9-40 所示报错，可以判定存在多余磁盘挂载点。



图 9-40　存在多余磁盘挂载点报错

统计出节点所拥有的数据磁盘的数量,通过 rm -rf 命令删除多余挂载点目录。

```
root@HZ-CAS01-CVK01:/opt/mds/disk# rm -rf 3/
root@HZ-CAS01-CVK01:/opt/mds/disk# rm -rf 4/
```

(4) 删除数据磁盘内数据

零存储集群添加节点时,必须保证节点内数据磁盘没有数据,否则无法将节点加入集群。通过"rm -rf /opt/mds/disk/*/*"命令删除所有挂载点的数据。

```
root@HZ-CAS01-CVK01:/opt/mds/disk# rm -rf /opt/mds/disk/*/*
```

(5) 检查 UMP 界面配置

在 UMP 界面添加节点时要求输入 IP 地址,此地址必须为存储内网 IP,如果输入其他网段地址会导致节点无法正常加入。

如果有如图 9-41 所示报错,可以判定为 IP 地址输入错误。



图 9-41　IP 地址输入错误报错

输入正确的存储内网 IP 地址。

(6) 检查虚拟共享存储配置

虚拟共享存储和零存储都需要使用 3260 端口，存在冲突，因此不能共存。运行零存储之前需要保证虚拟共享存储未开启，通过"service tgt status"命令查看虚拟共享存储的状态

```
root@HZ-CAS01-CVK02:~# service tgt status
tgt start/running, process 28118
```

如果输出如上述状态，则表示已经开启虚拟共享存储。

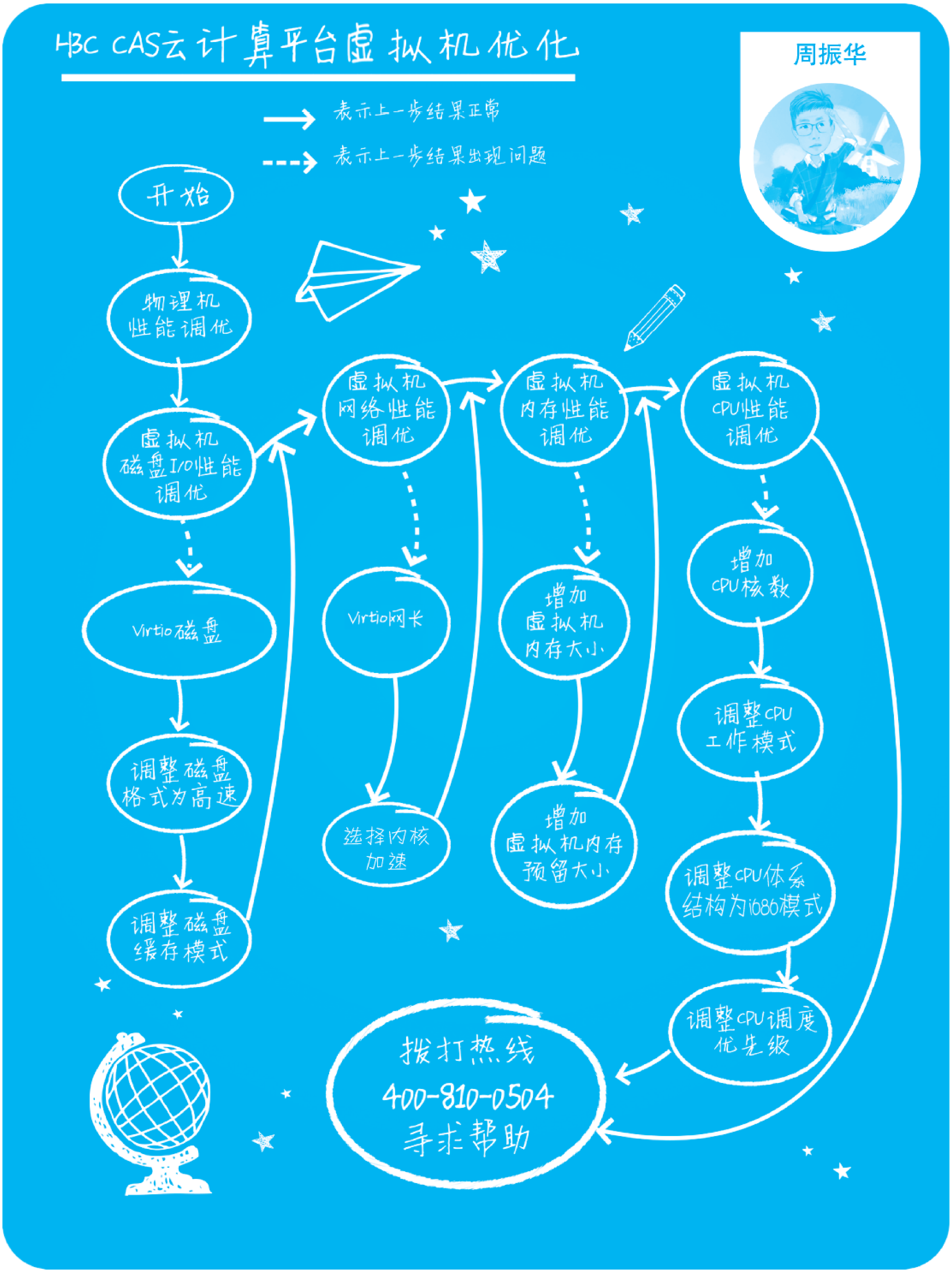
如果有如图 9-42 所示报错，也可以判定 3260 端口被占用。



图 9-42　3260 端口被占用报错

登录 CAS 管理平台删除虚拟共享存储，然后在后台输入命令"service tgt stop"，停止 tgt 服务，并删除虚拟共享存储配置文件 targets.conf 和 tgt.conf。

```
root@HZ-CAS01-CVK02:~# service tgt stop
tgt stop/waiting
root@HZ-CAS01-CVK02:~# rm /etc/tgt/targets.conf
root@HZ-CAS01-CVK02:~# rm /etc/init/tgt.conf
```


H3C CAS云计算平台虚拟机优化
周振华
表示上一步结果正常
表示上一步结果出现问题
开始
物理机性能调优
虚拟机磁盘I/O性能调优
Virtio磁盘
调整磁盘格式为高速
调整磁盘缓存模式
虚拟机网络性能调优
Virtio网卡
选择内核加速
虚拟机内存性能调优
增加虚拟机内存大小
增加虚拟机内存预留大小
虚拟机CPU性能调优
增加CPU核数
调整CPU工作模式
调整CPU体系结构为i686模式
调整CPU调度优先级
拨打热线
400-810-0504
寻求帮助

1. 开始

云计算平台虚拟机业务系统反应慢、延迟高涉及方方面面的因素，首先需要进行定位，确认造成慢的可能原因，然后根据原因针对性的进行调整。

① 确认业务系统在处理过程中的操作系统运行状态，查看虚拟机 CPU、内存、磁盘 I/O 和网络 I/O 的运行情况，看是否有哪些指标达到系统瓶颈。

② 确认业务系统在处理过程中的虚拟化平台运行状态，查看主机 CPU、内存、磁盘 I/O 和网络 I/O 的运行情况，看是否有哪些指标达到系统瓶颈。

③ 确认业务系统在处理过程中的软件运行状态，如 Web、中间件和数据库的连接数、上下文切换数等参数是否正常，有没有异常偏高。

④ 服务器工作在高性能模式下可以使虚拟机的系统更优，例如 R390/590 系列在 iLO 下如图 9-43 所示设置为 HP Static High Performance Mode。

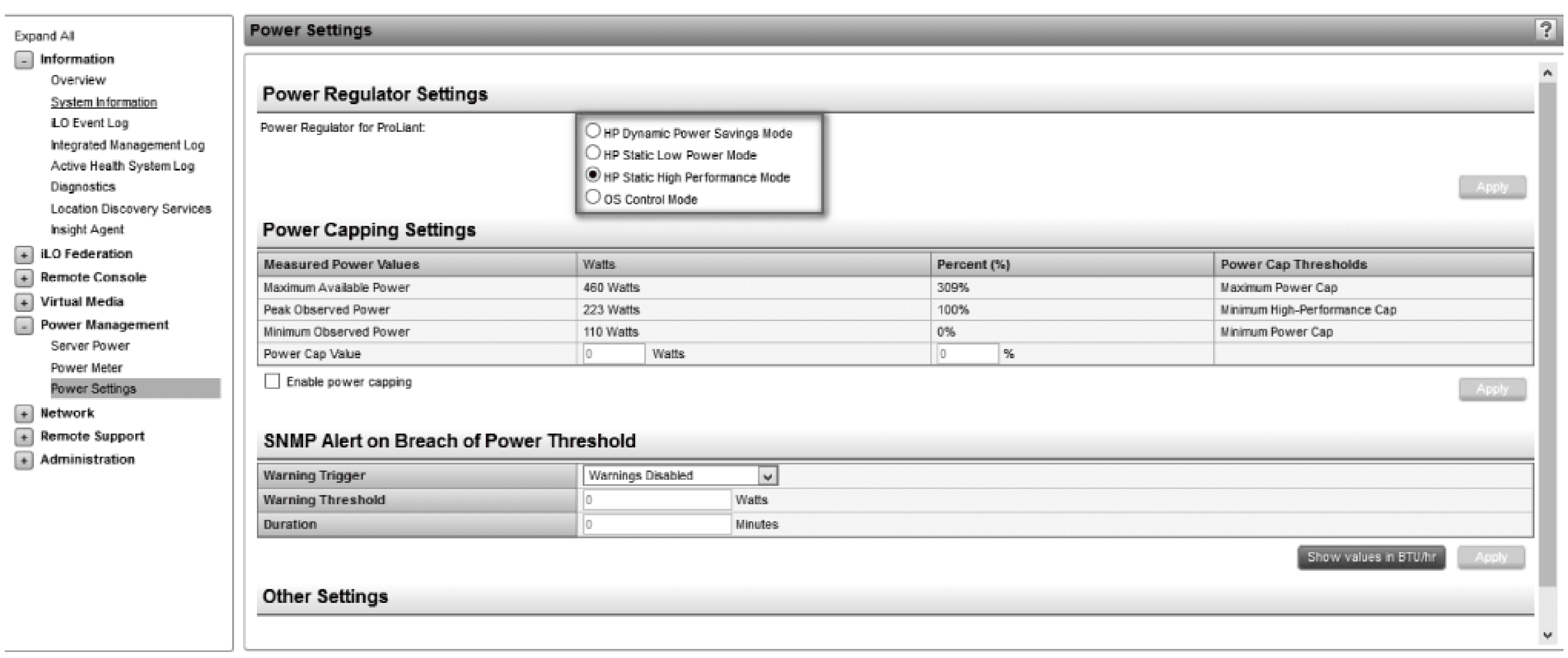


图 9-43 设置 R390/590 系列服务器模式

2. 流程图相关操作说明

（1）物理机性能调优

磁盘的 I/O 性能影响虚拟机数据的读写性能，物理服务器可以使用下面的方法进行调整。

① 使用服务器 raid 缓存卡：缓存卡可以有效提升部分重复性读写动作的性能，同时注意缓存卡一般可以配置读写缓存比例，可根据实际业务系统需要调整。

② 使用合适的外接存储：从 I/O 吞吐和延迟上，通常单业务系统性能比较结果为 FC 存储→IP 存储→分布式存储。分布式存储在拥有分布式计算系统或大量虚拟机业务并发的情况下可以有较优异表现，但无法在虚拟机单机业务系统中达到传统存储的级别。

③ 使用合适的外接存储连接方式：通常情况下，使用 FC 或 IP 的直通方式将 LUN 资源挂接到虚拟机业务系统上会较通过虚拟化平台文件系统转换得到更高的性能；但是不能实现 CAS 系统上快照、迁移等便利的虚拟化能力。

④ 使用更快速的磁盘：无论是服务器的本地磁盘还是外接存储的磁盘，SSD 类型速度远好于 SAS 和 SATA。

网卡性能影响虚拟机的网络传输速度，物理服务器的调优方法如下。

① 使用高速网卡：万兆好于千兆，光口稳定性好于电口。

② 选择合适的链路捆绑方案：服务器与交换机采用链路捆绑时，需对应选择动态或静态捆绑方式，并注意链路连接是否有问题。

服务器内存调优手段如下。

① 使用大内存：充足的物理服务器内容预留可以有效保障业务系统的内存使用性能。

② 使用带寄存器的内存型号：PC3L 类型内存较 PC3 类型内存增加了寄存器，速度更快。

服务器 CPU 调优手段如下。

① 取消物理服务器 CPU 以节能模式运行：部分新型号的物理服务器 CPU 会默认以节能模式运行，导致性能测试中短时间内无法达到较高结果，可以在 BIOS 中取消相关选项达到提升性能的测试效果。

② 使用较高频率的 CPU 型号服务器：部分业务系统设计只能使用有限的 CPU 核数，此时更多核数无意义，但主频 3.0 较 2.0 就会有很显著提升。

(2) 虚拟机磁盘 I/O 性能调优

虚拟机磁盘性能调优包括：磁盘类型、磁盘格式、磁盘缓存等。

(3) Virtio 磁盘

Virtio 是虚拟化技术针对 KVM 虚拟化平台优化的驱动类型，I/O 性能较 IDE 格式磁盘有极大提升。IDE 磁盘变更为 Virtio 磁盘的步骤是：在"修改虚拟机"中将原 IDE 磁盘删除，然后重新添加虚拟机磁盘文件，磁盘类型选择 Virtio 即可，如图 9-44 所示。



图 9-44 "修改虚拟机"对话框

（4）调整磁盘格式为高速

高速磁盘较智能磁盘在频繁 I/O 读写操作中表现更优，因此推荐使用高速磁盘模式。但高速模式在初始时就会占用所有设定的虚拟磁盘空间大小；高速模式只能在虚拟机关机情况下修改。

（5）调整磁盘缓存模式

磁盘缓存有 4 种模式。

Writeback：数据先经过 qemu 的缓存，再经过宿主机缓存，最后写往宿主机磁盘。

None：数据先经过 qemu 进程的缓存，然后写往宿主机磁盘。

Writethrough：数据先经过宿主机缓存，然后写往宿主机磁盘。

Directsync：数据直接写往宿主机磁盘。

从读写性能来比较：Writeback→None→Writethrough→Directsync，但实际上由于 Writeback 增加了缓存级别，导致故障时丢数据的风险增加，因此不适用于数据库等较敏感业务系统（大量缓存数据丢失可能会导致数据库同步异常进而出现崩溃）。

（6）虚拟机网络性能调优

虚拟机网络性能调优包括网卡类型、内核加速等。

（7）Virtio 网卡

Virtio 是虚拟化技术针对 KVM 虚拟化平台优化的驱动类型，I/O 性能较其他类型网卡有极大提升。

修改后网卡信息如图 9-45 所示。

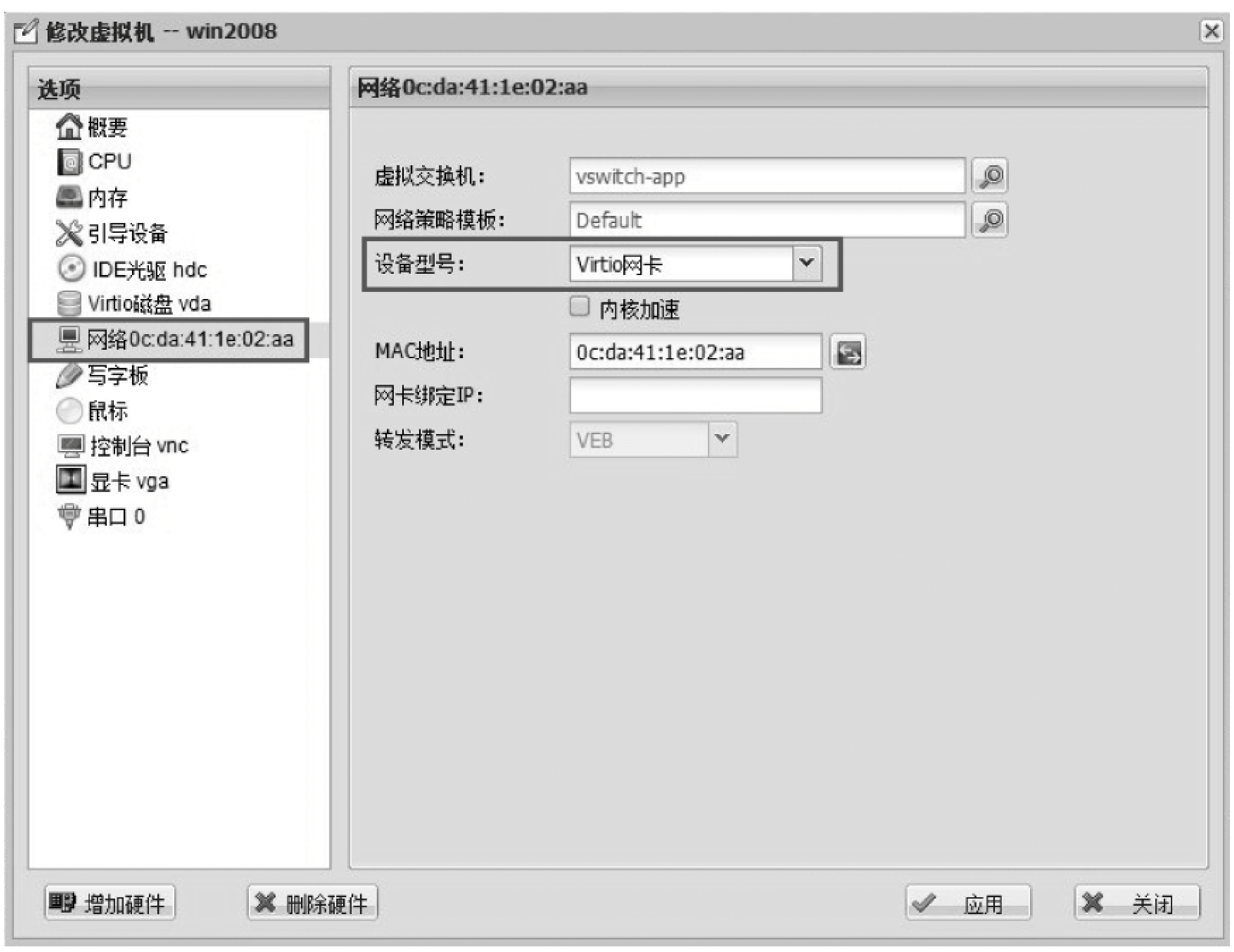


图 9-45　修改后网卡信息

（8）选择内核加速

在部分网络性能测试场景下，选择内核加速可以有效优化测试结果，使虚拟网卡能够接近

万兆线速转发能力。在关闭虚拟机的状态下勾选“内核加速”复选框,如图 9-46 所示。



图 9-46　选择内核加速

(9) 虚拟机内存性能调优

虚拟机内存性能调优包括:适当调整虚拟机内存大小、增加虚拟机内存预留大小等。

(10) 增加虚拟机内存大小

当虚拟机内存使用率高时,可以通过增加虚拟机内存大小调优。

(11) 增加虚拟机内存预留大小

内存预留的作用是强制该虚拟机在启动后马上分配所预留的内存,该内存只给这台虚拟机使用。调整内存预留大小可以对内存切换较为频繁的业务系统有提升性能的效果,尤其是存在多虚拟机抢占内存的场景下,如图 9-47 所示。

(12) 虚拟机 CPU 性能调优

CPU 性能调优包括:适当增加 CPU 核数、调整 CPU 工作模式、调整 CPU 体系结构、CPU 调度优先级等。

(13) 增加 CPU 核数

当虚拟机业务系统具备多核处理计算能力时可以有效提升性能,如图 9-48 所示。

(14) 调整 CPU 工作模式

虚拟机的 CPU 工作模式有 3 种。

① Custom:qemu 虚拟出的 CPU。CAS 默认使用该模式,CPU 默认为 qemu64 类型,兼容性好,但因支持的指令少,导致某些性能低,如 AES 加密等。

② Host Model:启动虚拟机前,从 qemu 能够模拟出的 CPU 中找一个和主机 CPU 最接近的型号,迁移兼容性较差,amd 和 intel 之间不能迁移。

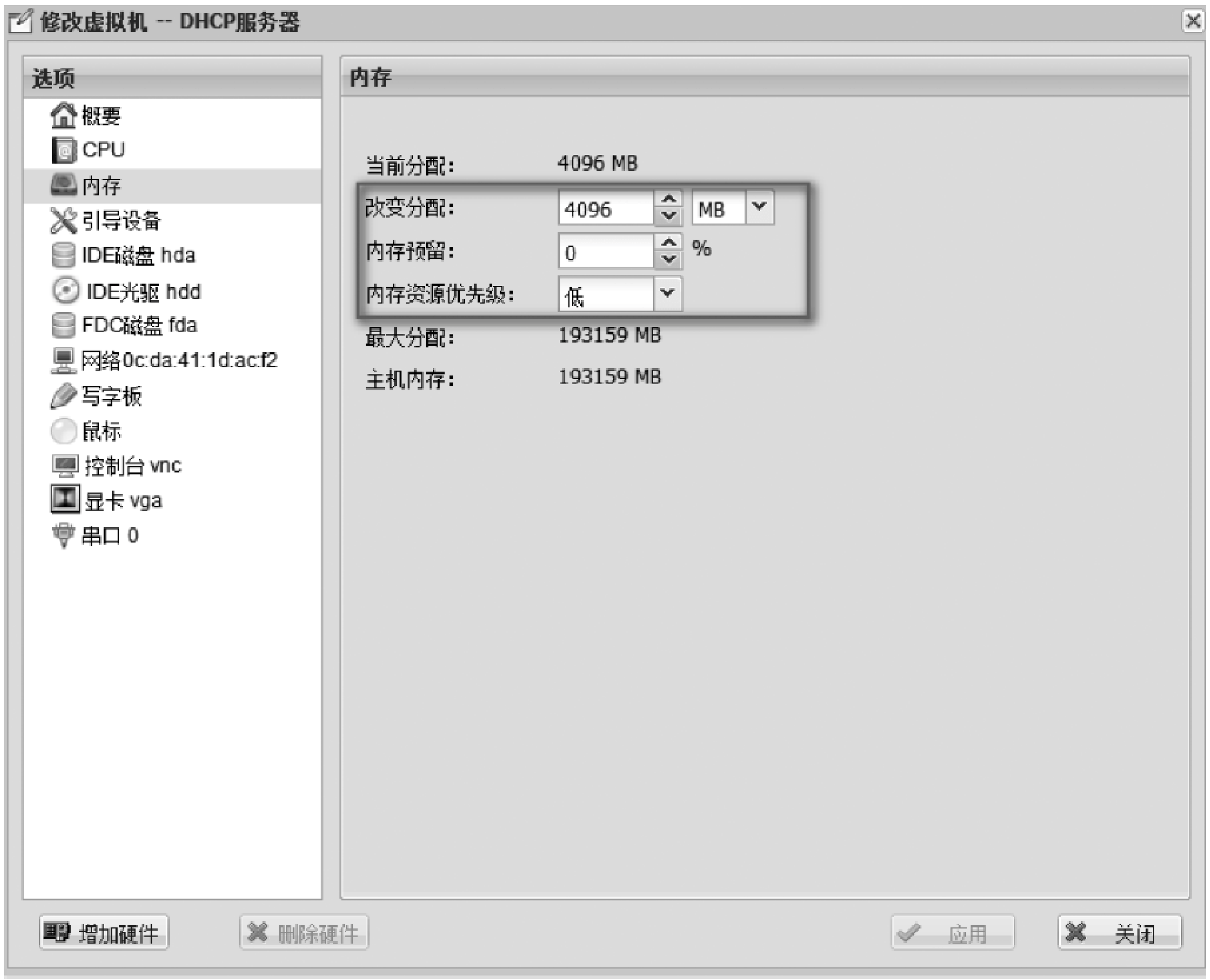


图 9-47　虚拟机内存预留大小调整



图 9-48　增加 CPU 核数

③ Host Passthrough：直接透传主机 CPU 型号和大部分功能给虚机，迁移兼容性差。CPU 特性完全相同的主机间才可以迁移，同一厂家不同代的 CPU 之间也不能迁移。

性能方面 Host Passthrough→Host Model→Custom，但兼容性 Custom 最好，Host Passthrough 最差。具体场景需要视物理服务器使用的物理 CPU 型号支持的加速能力而定。

CUP 工作模式选择 Custom，如图 9-49 所示。



图 9-49 选择 Custom 工作模式

(15) 调整 CPU 体系结构

某些虚拟机业务性能方面在单核或虚拟机操作系统为 i686 格式时较好，如图 9-50 所示，比如：某局点的 Webloigc 9.2 版本中使用的 java 版本是 jdk150_04。



图 9-50 调整 CPU 体系结构

（16）调整 CPU 调度优先级

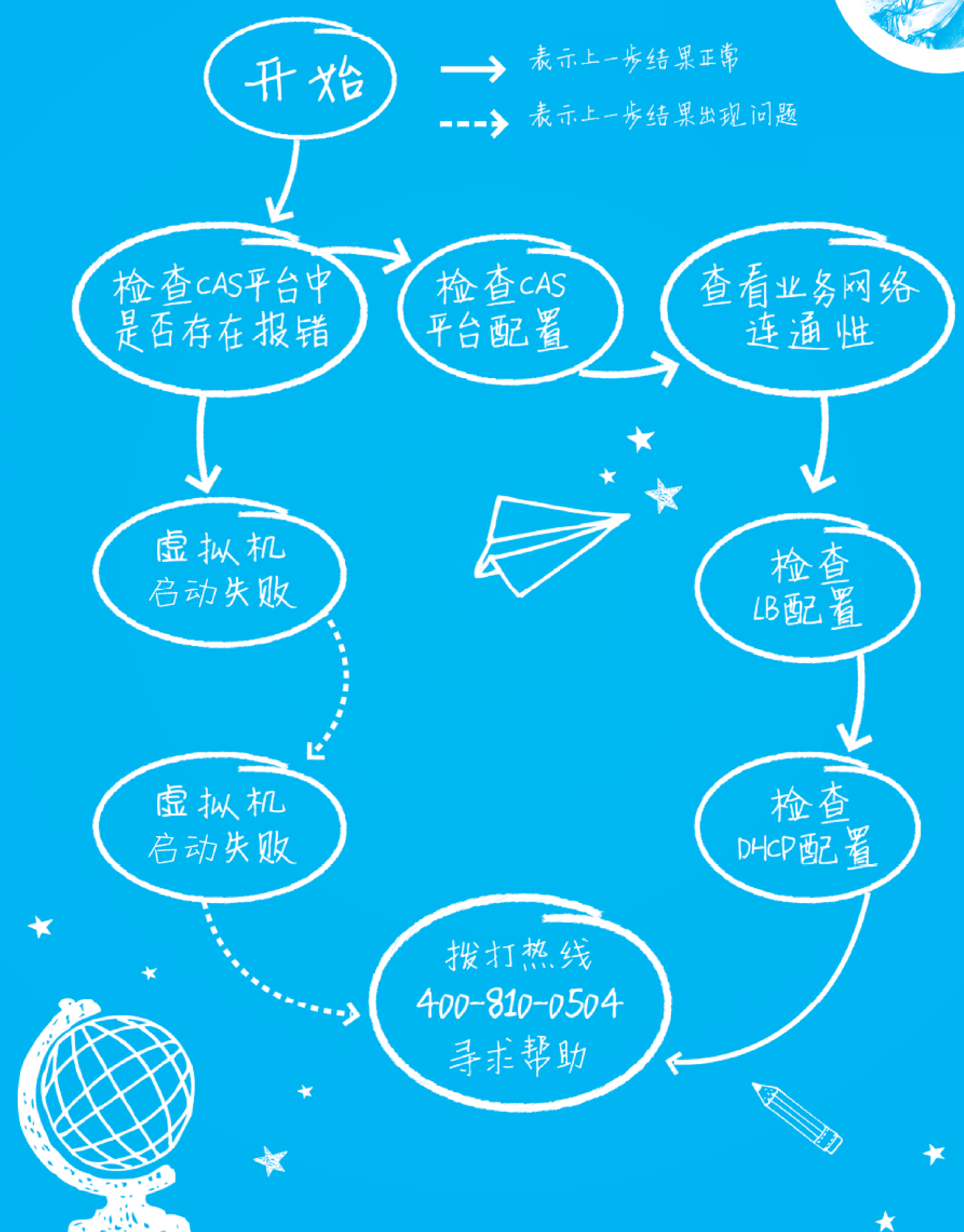
当存在较多虚拟机同时抢占 CPU 时，可以有效提升高优先级的处理。重要虚拟机业务调整高优先级，如图 9-51 所示。



图 9-51 调整 CPU 调度优先级

DRX业务扩展故障排查

厉梦如



1. 开始

DRX 动态资源扩展业务在扩展业务虚拟机时，有多种原因导致业务虚拟机无法正常扩展或者扩展出的虚拟机不可用。问题大致可以分为以下 3 大类。

① CAS 配置存在错误。

② 物理主机资源不足。

③ 网络配置存在错误。

根据故障的具体现象，可根据如下的思路进行定位。

① 查看 CAS 平台中是否存在报错提示信息，根据报错信息进行排查。

② 查看 CAS 动态资源扩展配置。

③ 检查交换机、LB 等设备上网络配置。

2. 流程图相关操作说明

（1）检查 CAS 平台中是否存在报错

当出现动态扩展业务虚拟机异常，排查时建议先登录 CAS 平台在操作日志中查看是否存在报错信息，以便利用报错信息更快判定具体的问题原因。

如图 9-52 所示，查看 CAS“操作日志”，DRX 问题的报错信息中：“操作员姓名”一栏中应该为 system 代表此操作是系统根据监控策略自动触发的。“操作描述”中会对具体的扩展、启动虚拟机动作进行描述。

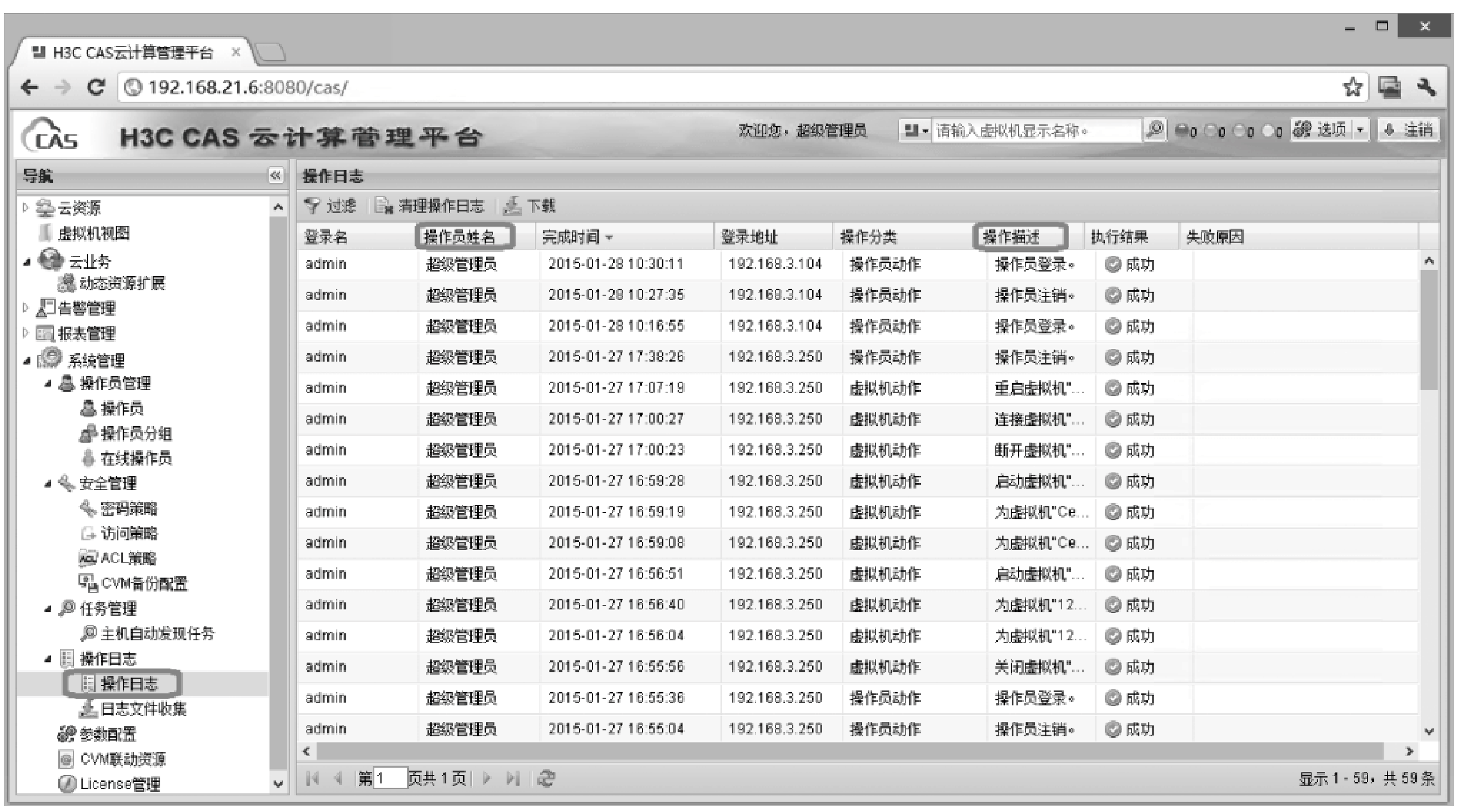


图 9-52　CAS“操作日志”

（2）虚拟机部署失败

如果在 CAS 平台的操作日志中查看到有报错信息为虚拟机部署失败，主要有以下几种原因。

① 存在同名虚拟机或者目的存储池已有同名虚拟机文件，报错信息为“虚拟机文件已存在”。

② 存储空间不足，虚拟机镜像文件无法正常部署，报错“虚拟机部署失败”。

③ 虚拟机模板存在问题，虚拟机无法正常部署，报错“虚拟机部署失败”。

针对相应报错对症下药，药方见下。

报错信息“虚拟机文件已存在”：先在 CVK 主机上的“存储”选项卡查看是否确实已经存在同名虚拟机，并在目的存储池中查看是否有相应名称的虚拟机文件，如图 9-53 所示。如果有同名虚拟机及相应文件请协调删除或更改动态资源扩展配置中的虚拟机名称。



图 9-53 报错信息“虚拟机文件已存在”

报错“虚拟机部署失败”：首先查看目的共享存储池的可用空间是否有足够存储资源供扩展虚拟机，如图 9-53 所示。如果可用的存储资源足够，则排查 DRX 策略中对应的虚拟机模板是否存在，如图 9-54 所示。



图 9-54 虚拟机模板排查

如果模板存在且物理机可用存储资源充足，尝试用该模板手工部署一台虚拟机，并观察其运行情况以确认虚拟机模板是否正常。如果手工部署虚拟机也失败，则虚拟机模板本身很可能存在问题。

如果手工部署的虚拟机能够正常启动并提供服务，则模板本身也没有问题。那么需要查看下模板部署出的虚拟机是否挂载有 ISO 镜像、PCI 设备、USB 设备等。如果存在单击“修改虚拟机”命令，并在界面中使用“删除设备”删除掉这些设备，并在 IDE 光驱里将相应挂载的 ISO 文件取消掉，重新制作虚机模板，如图 9-55 所示。



图 9-55 “修改虚拟机”对话框

说明：虚拟机模板中 IP 地址一项必须设置为自动获取，对于 Linux 系统的虚拟机在制作模板前还需注意将网卡信息文件进行删除，如 ubuntu 系统中的网卡信息文件为存储在/etc/udev/rules.d 目录下的 70-presistent-net.rule 文件。

(3) 虚拟机启动失败

CAS 平台上的报错提示包含“虚拟机启动失败”内容，请注意具体报错信息提示。

出现如图 9-56 所示的系统调用失败可查看是否有相应的 USB 设备、ISO 光盘等。

需要确保物理宿主机性能足够，如 CPU、内存资源足够才可确保虚拟机扩展处能够正常启动。

如果以上步骤排查完毕后，仍然无法判定故障原因，请联系热线 400-810-0504 进行处理。

(4) 检查 CAS 平台配置

CAS 平台操作日志没有发现报错，下一步就是确认动态资源扩展业务配置正确。

① 确认动态资源扩展业务已经正常生效。

在相应“动态资源扩展策略”对话框，修改相应动态资源策略，确认“立即生效”已经勾选，确保动态资源扩展业务已经生效，如图 9-57 所示。



图 9-56　系统调用失败

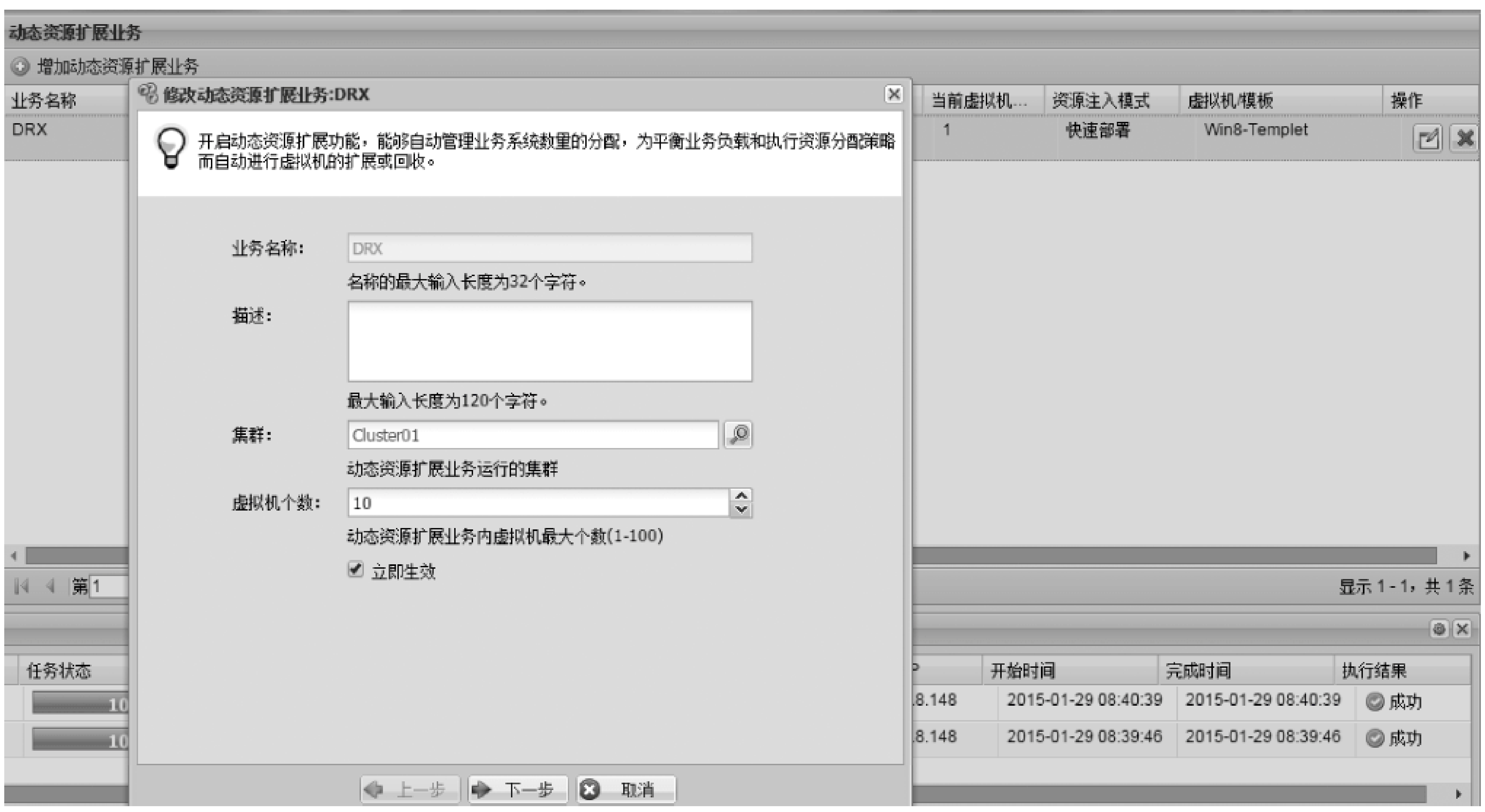


图 9-57　确认动态资源扩展业务已经正常生效

确认业务虚拟机组中已包含所有承载业务的虚拟机，如图 9-58 所示。如果虚拟机组中未包括任何虚拟机，则 DRX 无法正常工作。

② 确认 CAS 上配置地址段与交换机上 DHCP 池没有冲突。

查看交换机上是否有 DHCP 配置，如果已经有配置，CAS 上请勿配置相应地址段。如果之前在交换机上未有相应配置，请检查设置的网段地址是否准确。

③ 检查资源扩展策略的设置。

检查资源扩展策略中的监控参数的设置，确认现有业务虚拟机的性能监控界面显示的实时性能指标是否已经超过监控策略设置的阈值。如果阈值设置过高，则现有业务虚拟机很难扩展，请按照实际业务情况调整，如图 9-59 所示。

(5) 查看业务网络连通性

在之前步骤均未发现异常的情况下，请排查网络。



图 9-58　“修改动态资源扩展业务”对话框

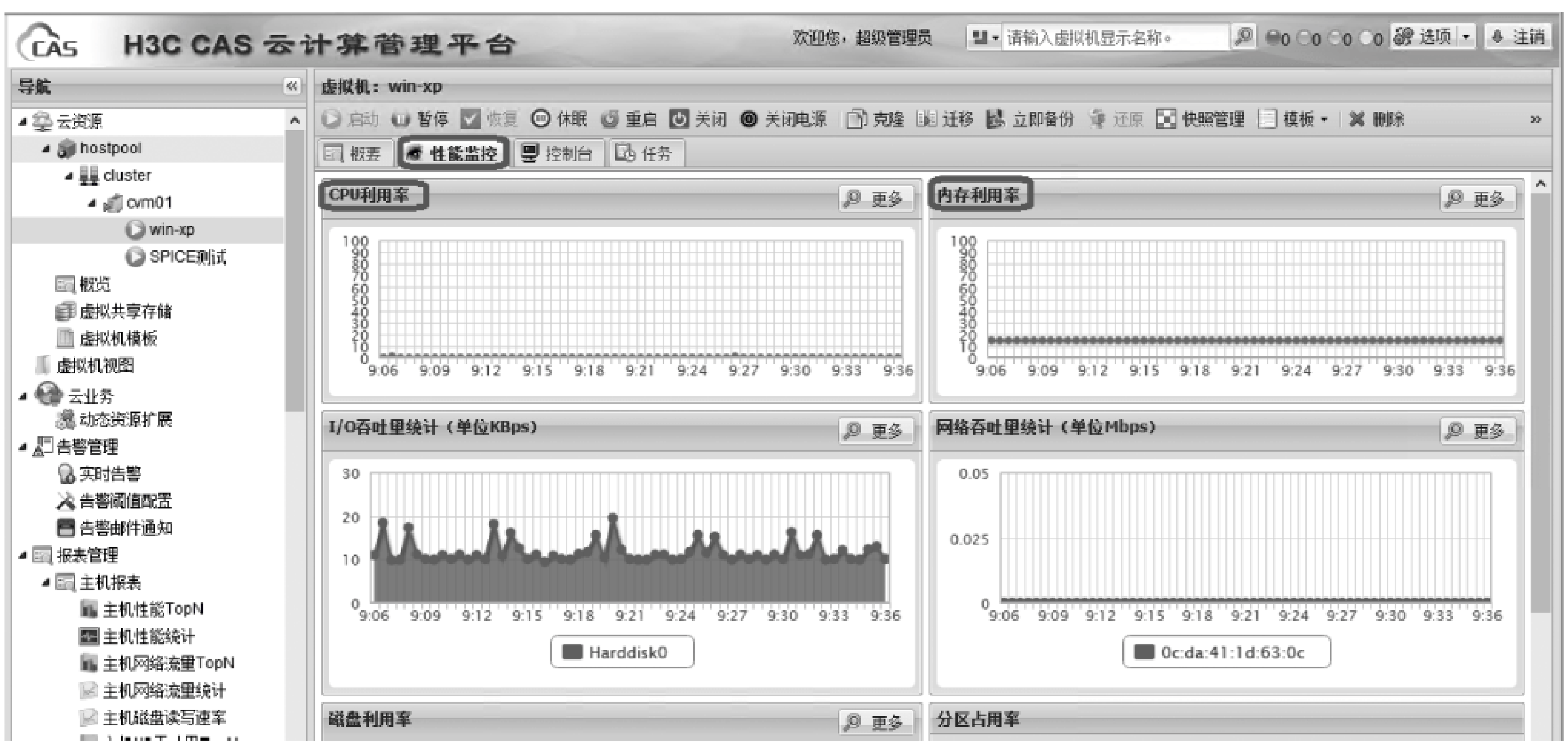


图 9-59　虚拟机性能监控界面

① 外部访问地址到 LB 上虚 IP 地址之间的连通性。

② LB 到各个业务虚拟机之间的 IP 连通性。

③ 检查其他网络连通所需的必须配置，如 NAT 配置等是否正常。

(6) 检查 LB 配置

Web 方式登录 LB 的配置界面确认其配置正确，以免因为服务器负载分担设置错误导致扩展出的虚拟机无法正常承载业务。

① 查看 LB 上实服务的配置情况，如图 9-60 所示。



图 9-60　实服务配置情况

(a) 实服务地址必须包含所有业务虚拟机的地址。

(b) 确保所有实服务均正确加入业务实服务组。如果配置正常生效，已经启动的业务虚拟机的状态应为绿色正常工作。

② 检查实服务组的配置。

(a) 确保实服务使用了合理的算法将业务平均分发到各个业务虚拟机上。

(b) 根据业务需求调整健康性检测的检测方法，健康性检测通过条件，如图 9-61 所示。

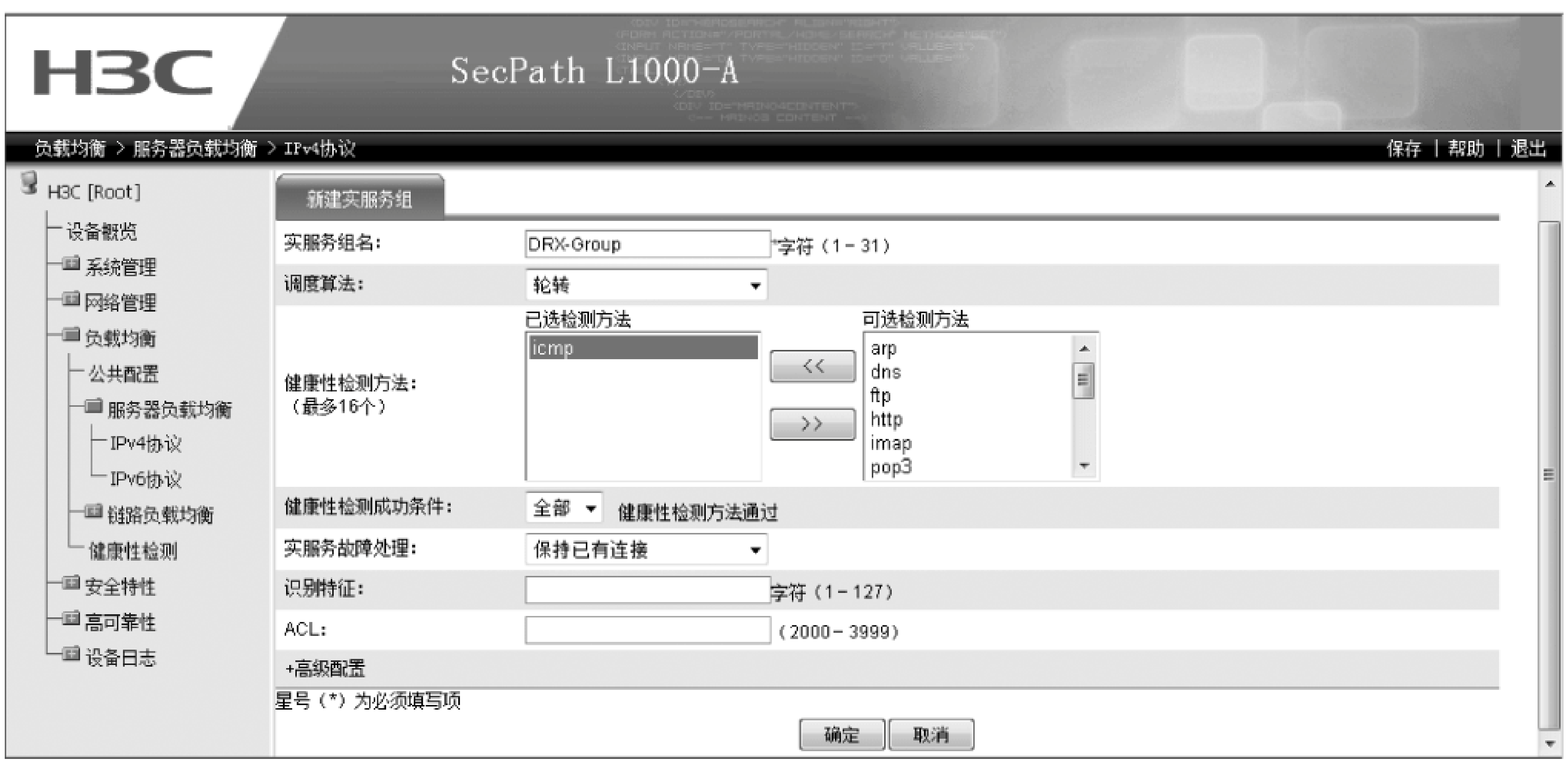


图 9-61　调整健康性检测

③ 检查虚服务的配置，如图 9-62 所示。

(a) 注意虚服务地址是否设置正确，并根据 LB 在网络环境中的组网情况判断是否需要使能 SNAT 功能。

(b) 特别注意确保虚服务本身已经使能，如没有使能则服务器负载分发功能不会正常工作。



图 9-62 虚服务的配置

（7）检查 DHCP 配置

查看为 DRX 业务虚拟机提供 DHCP 服务的地址池，确认其中包含所有业务虚拟机的地址，并确认 DHCP 服务正常。

说明：从 CAS E0201 版本开始，DRX 业务可以在 CAS 的 Web 界面进行配置扩展虚拟机 IP 地址段，网络设备上的 DHCP 已经非解决方案里的必备选项，因此在排查时请先确认方案中规划了使用网络设备给虚拟机分配地址。如不涉及，可略过此步骤。

如果排查过均未发现异常，DRX 本身配置应无问题。由于 DRX 业务正常承载业务还需业务系统正常支持，建议协调业务系统厂商进行排查。如对动态资源扩展方案还有疑惑，请联系热线 400-810-0504 进一步分析。

虚拟机手动迁移失败故障排查

厉梦如





1. 开始

虚拟机手动在线迁移应用场景发生在管理员日常运维或巡检时，手工对虚拟机的运行载体(包括计算资源和存储资源)进行变更，以达到系统运行最优化的目的。比如需要对主机进行硬件升级时，可以利用手工迁移方式，将原本运行在该主机上的虚拟机前部迁移到其他正常工作的主机上，然后再对该主机进行关机断电处理，完成之后，再将虚拟机手工迁移回来。在手工迁移过程中，触发虚拟机迁移的动作是人为控制的，迁移存储花费的时间又与磁盘实际使用时间、存储迁移网络带宽等有密切关系。

虚拟机迁移失败，在 CAS 平台的任务台会显示相应报错。根据迁移的不同方式和报错，可初步判断以下 4 类故障类型。

① 虚拟机磁盘格式非 qcow2 文件格式不支持在线迁移存储。

② 虚拟机挂载虚拟光驱、USB 设备、软驱、串口设备等。

③ 虚拟机磁盘文件存放在本地目录。

④ 虚拟机迁移目的主机没有挂载相同的存储池或者虚拟交换机。

因此虚拟机在线迁移失败的排查思路。

① 虚拟机磁盘格式是否为 qcow2 格式。

② 虚拟机有没有挂载虚拟光驱、USB 等。

③ 排查虚拟机磁盘文件是否都在共享存储上。

④ 确认迁移的目的主机是否挂载了相同的存储池、配置相同的虚拟交换机。

2. 流程图相关操作说明

(1) “更改数据存储”功能不可用

虚拟机在线迁移数据存储，发现“更改数据存储”功能被置灰不可用，如图 9-63 所示。出现该问题原因是虚拟机磁盘格式非 qcow2 格式，如图 9-64 所示 CAS 不支持非 qcow2 格式磁盘的虚拟机在线迁移数据存储，需要更改迁移方式。

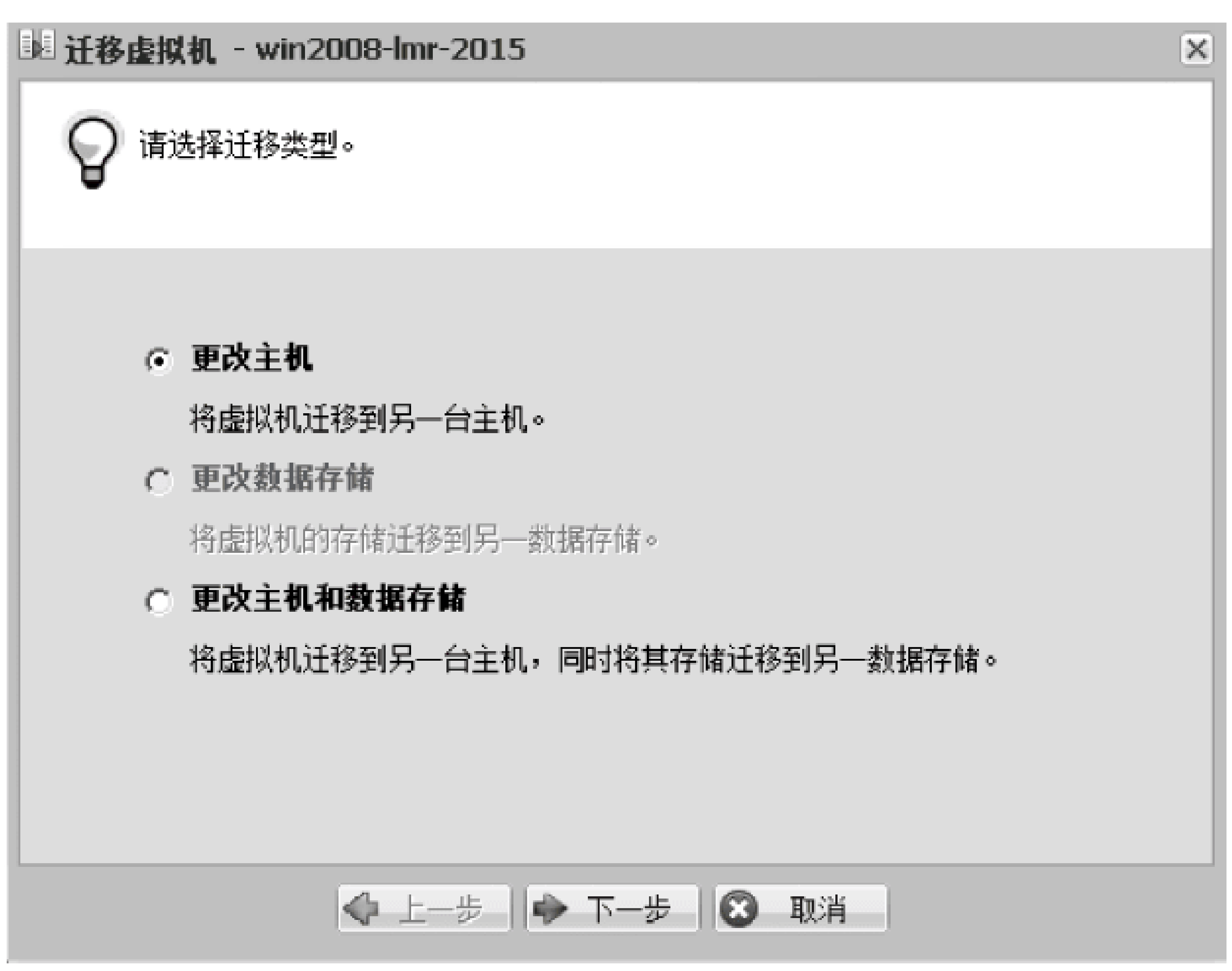


图 9-63 虚拟机在线“更改数据存储”功能不可用



图 9-64　虚拟机磁盘类型为 raw，非 qcow2

说明：CAS 平台的虚拟机支持使用 qcow2 和 raw 格式磁盘，分别对应创建磁盘文件时候的智能格式和高速格式，如图 9-65 所示。部分特性和功能只能在磁盘类型为 qcow2 的虚拟机上才能使用，比如虚拟机快照功能和如图 9-63 所示的在线“更改数据存储”。



图 9-65　虚拟机新增磁盘可设置磁盘类型

(2) 更改迁移方式

非 qcow2 格式磁盘的虚拟机支持使用以下方式迁移。

① 虚拟机在线或离线“更改主机”。

② 虚拟机离线“更改数据存储”。

③ 虚拟机在线或离线“更改主机和数据存储”。

所以如果需求仅为迁移虚拟机磁盘所在存储池，则可采用虚拟机离线方式迁移；如果需求为同时更改虚拟机所在主机和磁盘所在存储池，则虚拟机可在线选择“更改主机和数据存储”方式进行迁移。

(3) 虚拟机使用本地光驱/已挂载 USB 设备/软驱/串口设备等

虚拟机迁移失败，在 CAS 平台的任务台会显示相应报错。报错为虚拟机使用本地光驱、已经挂载了 USB 设备、软驱或者串口设备等不允许迁移，如图 9-66、图 9-67 所示，即表示虚拟机在迁移前所拥有的这些“硬件”在目的主机无法自动提供给该虚拟机，故虚拟机在迁移前将该类型“硬件”移除。

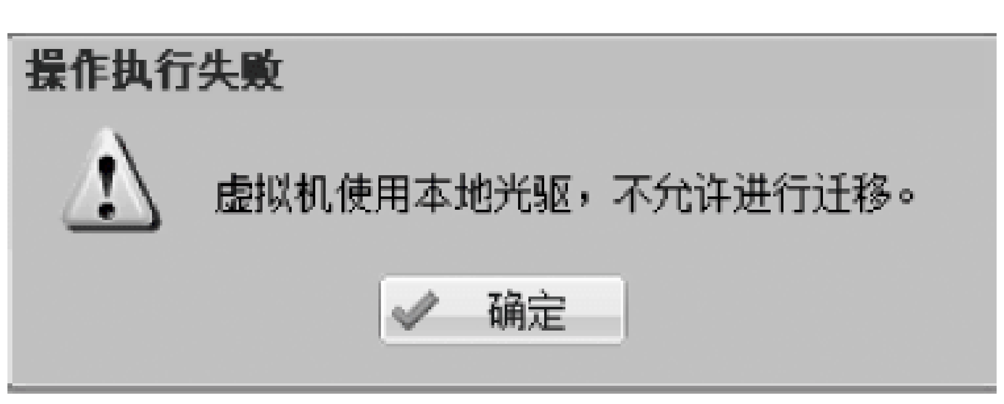


图 9-66　虚拟机使用本地光驱时不允许迁移

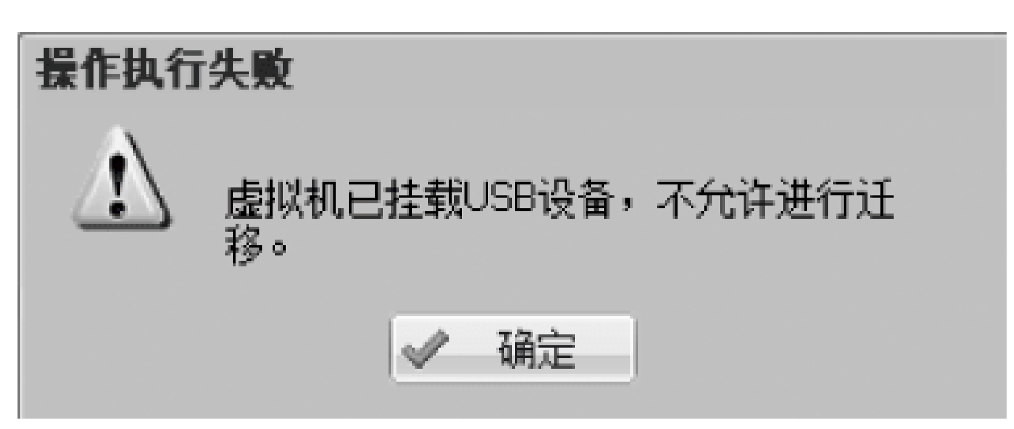


图 9-67　虚拟机挂载 USB 设备时不允许迁移

说明：如果有 USB 设备跨物理主机仍可以被虚拟机使用的需求，可以使用 USB over Network 等第三方技术。

（4）断开虚拟机“本地硬件”连接

断开虚拟机“本地硬件”连接需要在修改虚拟机界面操作。

如删除 USB 设备具体操作为：进入“修改虚拟机”对话框，选择“USB 设备”命令，然后单击“删除硬件”按钮，确认即可，如图 9-68 所示。

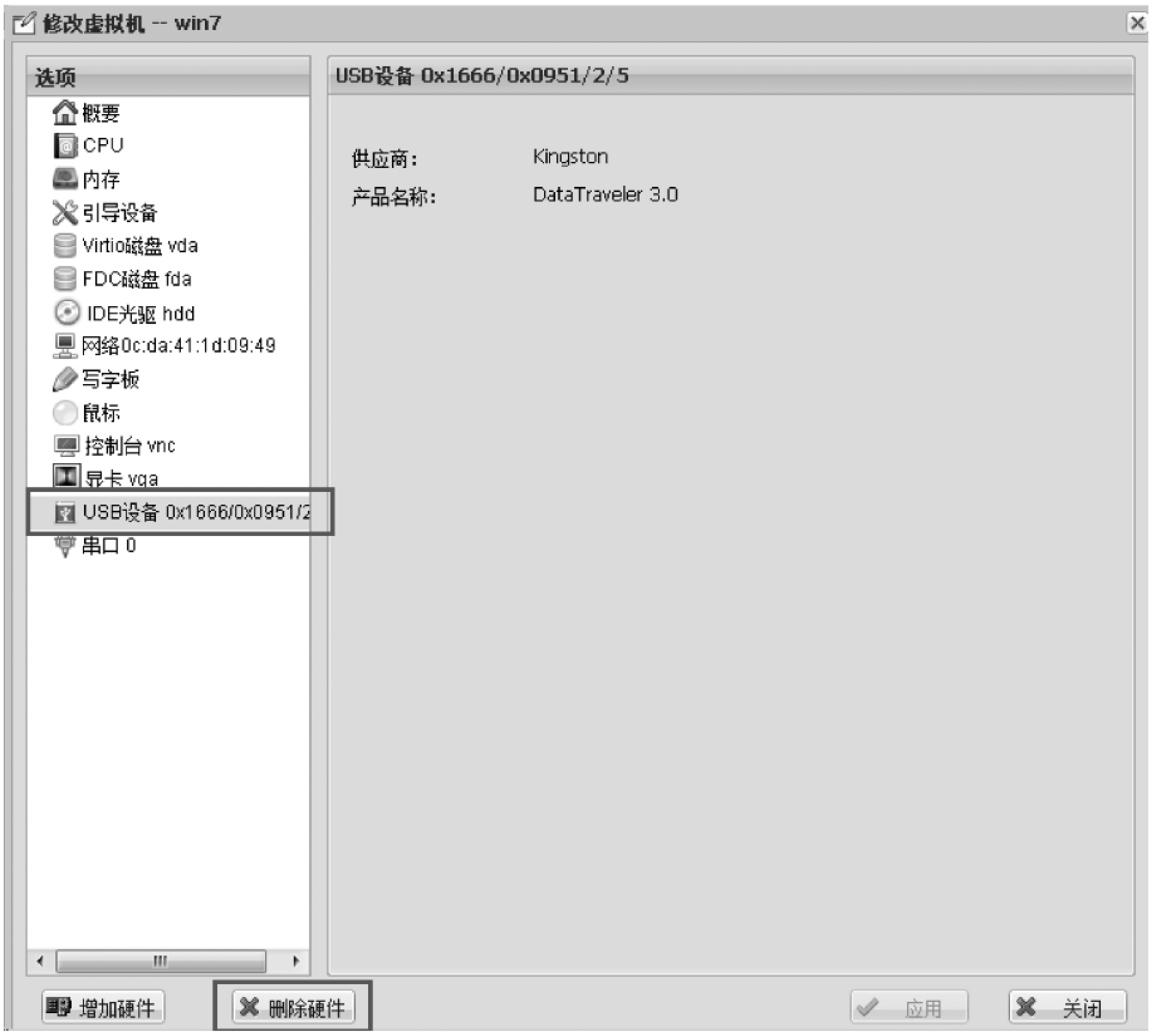


图 9-68　虚拟机删除挂载的 USB 设备

断开 IDE 光驱操作类似：进入“修改虚拟机”对话框，选择“IDE 光驱”命令，然后单击“断开连接”按钮，确认即可，如图 9-69 所示。

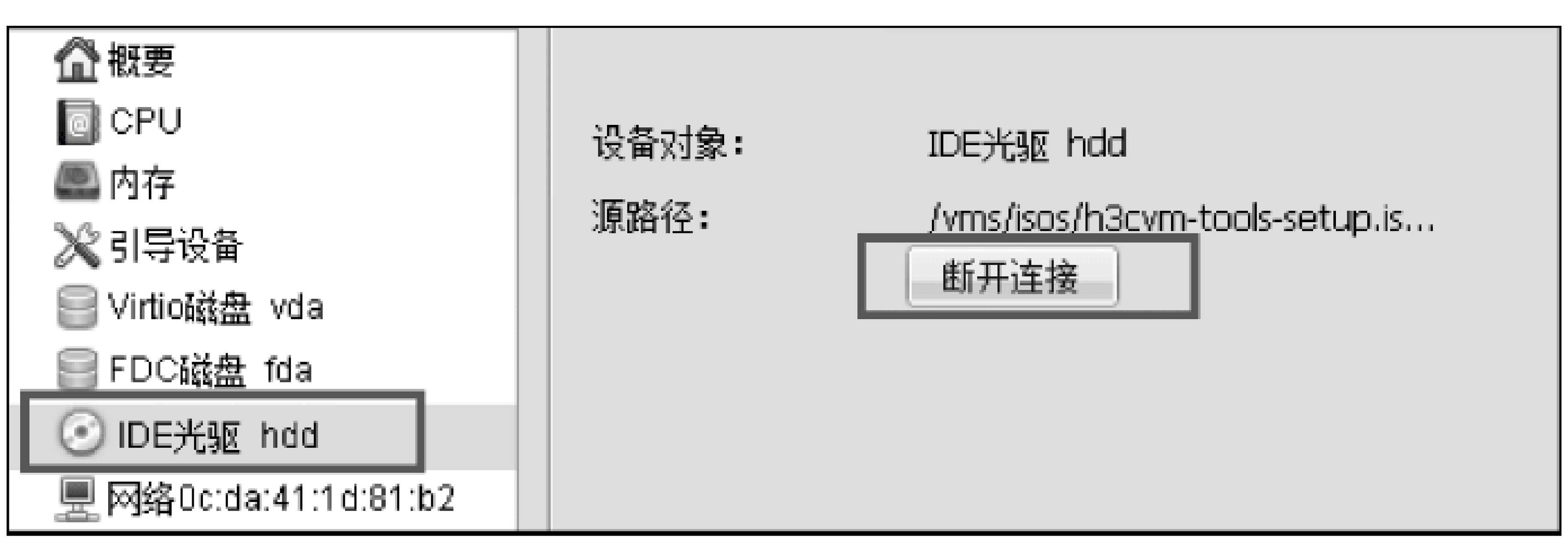


图 9-69　虚拟机断开本地光驱连接

（5）虚拟机使用本地存储或基础镜像文件

虚拟机的磁盘文件必须全部存储在共享文件系统上才允许在线更改虚拟机所在主机等，

一般出现该类报错原因如下。

① 虚拟机磁盘存储在本地存储目录，如图 9-70 所示。

② 虚拟机使用了多个磁盘，且部分或全部为本地磁盘。

③ 虚拟机的基础镜像文件部分或全部存储在本地存储目录，如图 9-71 所示。

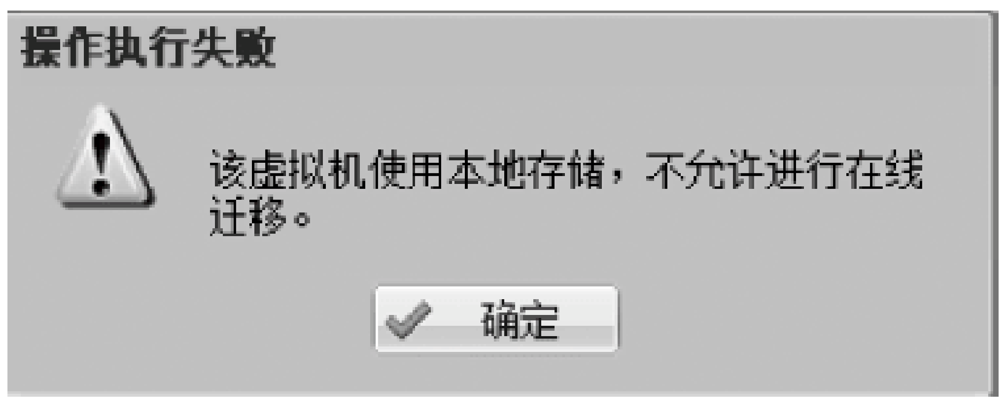


图 9-70 虚拟机使用本地存储时不允许在线迁移

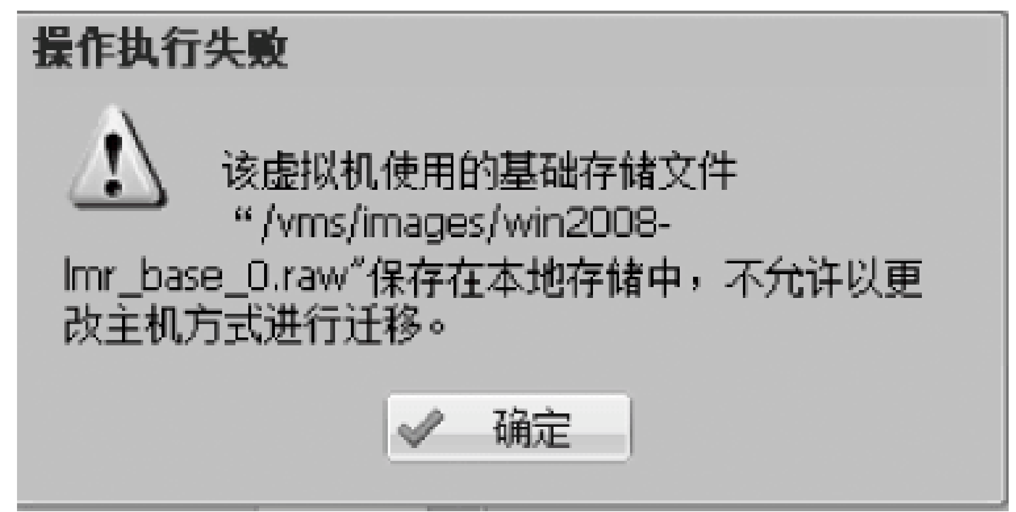


图 9-71 虚拟机基础镜像文件使用本地存储时不允许以更改主机方式进行迁移

(6) 更改迁移方式

查看虚拟机磁盘所在目录，如果出现以下 3 种类型，则需要虚拟机采用“更改主机和数据存储”选项迁移或者采用离线方式迁移。

① 虚拟机的磁盘存储在本地目录。

② 检查虚拟机的基础镜像文件 base0 或者 base1 的存储路径，其中有一个或者两个在本地。

③ 若虚拟机使用了多个磁盘，且其中有一个或多个为本地磁盘。

例如：如图 9-72 所示，查看该虚拟机存储信息，其中一个磁盘存储在/vms/images 的本地磁盘下，即需要采用“更改主机和存储”选项迁移或者离线迁移。



存储信息

	设备...	总线类型	存储卷路径	容量	类型	基础镜像文件
磁盘	hda	ide	/vms/sharefile/win2008-l...	48.83GB	文件	
磁盘	hdb	ide	/vms/images/win2008-l...	1000.00MB	文件	

图 9-72 虚拟机部分磁盘使用本地存储

(7) 目的主机不存在相应虚拟交换机或存储池等。

虚拟机迁移过程中会检测目的主机是否存在虚拟机需要的相应硬件资源。

① 虚拟机使用“更改主机”或者“更改主机和数据存储”所在主机时，虚拟机迁移过程中不会更改虚拟机网卡所在的虚拟交换机，如果目的主机没有相应的虚拟交换机，则不允许迁移，如图 9-73 所示。

② 虚拟机使用“更改主机”方式迁移时，虚拟机迁移过程中不会改变磁盘文件存储路径，如果目的主机没有相应的共享存储池，则不允许迁移，如图 9-74 所示。



图 9-73 不允许进行迁移

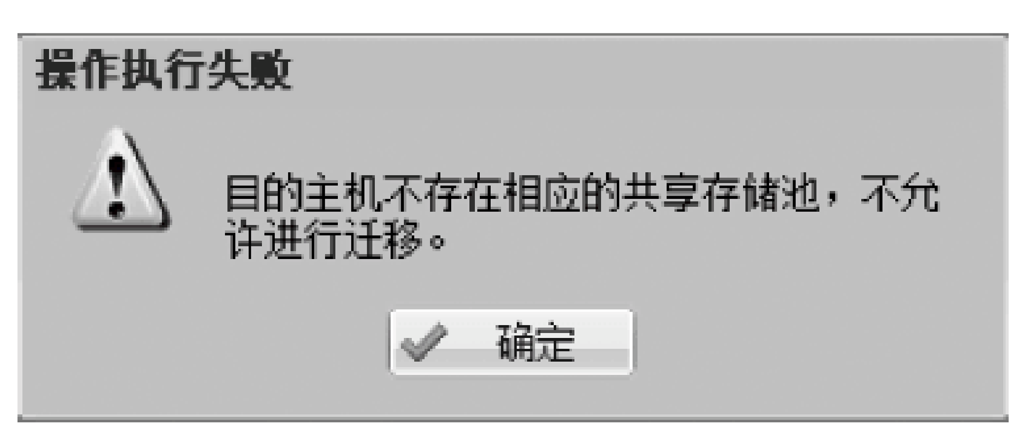
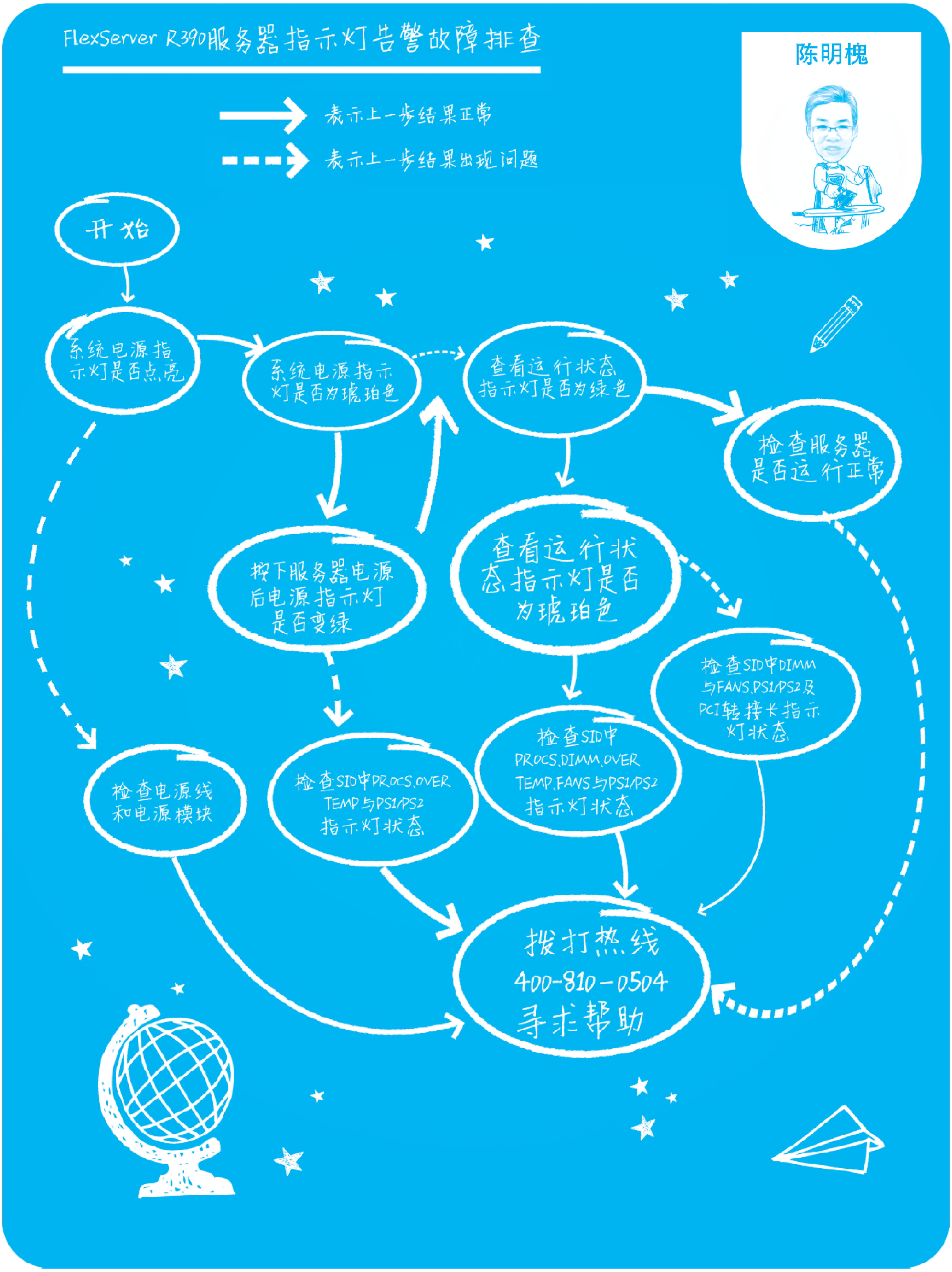


图 9-74 不存在相应的共享存储池

（8）目的主机增加相应配置或修改迁移方式

目的主机不存在虚拟机所需的硬件资源，可以通过在目的主机新建相应虚拟交换机或者挂载对应的共享存储池等来解决。如果出现目的主机无法增加相应共享存储池，也可以选择“更改主机和数据存储”或者虚拟机离线方式迁移。

以上方法如果仍无法解决问题，请联系 H3C 400-810-0504 处理。


FlexServer R390服务器指示灯告警故障排查
陈明槐
表示上一步结果正常
表示上一步结果出现问题
开始
系统电源指示灯是否点亮
系统电源指示灯是否为琥珀色
查看运行状态指示灯是否为绿色
检查服务器是否运行正常
按下服务器电源后电源指示灯是否变绿
查看运行状态指示灯是否为琥珀色
检查SID中DIMM与FANS.PS1/PS2及PCI转接卡指示灯状态
检查电源线和电源模块
检查SID中PROCS.OVER TEMP与PS1/PS2指示灯状态
检查SID中PROCS.DIMM.OVER TEMP.FANS与PS1/PS2指示灯状态
拨打热线
400-810-0504
寻求帮助

1. 开始

FlexServer R390 服务器前面板有诸多 LED 指示灯，当出现服务器开机故障时，可以通过 LED 指示灯显示信息判断服务器开机故障的原因。根据服务器指示灯的不同状态以及不同组合，可初步判断以下 6 种服务器故障。

① 服务器电源故障。

② 服务器处理器故障/缺失/不兼容。

③ 服务器内存故障。

④ 服务器风扇故障或已取下。

⑤ 服务器温度过高。

⑥ PCI 转接卡笼未正确就位。

因此服务器指示灯的排查思路。

① 若服务器接通电源后 LED 指示灯均不亮，排查电源模块是否插牢，替换电源线排除电源线故障。

② 检查系统电源 LED 指示灯。

③ 检查系统运行状况指示灯。

④ 检查 Source Insight(SID) LEDs 指示灯。

2. 流程图相关操作说明

(1) 系统电源指示灯是否点亮

如图 9-75 所示标号 1 为开机/待机按钮和标号 2 系统电源 LED 指示灯，查看指示灯是否点亮。

(2) 检查电源线和电源模块

检查电源线主要包括以下内容。

① 电源线是否故障，寻找其他电源线进行替换验证，确认电源线正常。

② 电源线是否松动。

③ 重新安装电源模块：电源模块安装没有正确就位，会导致服务器无法正常开机。因此先断开电源线，然后拔出并重新安装电源模块。

如果以上步骤执行完毕后系统电源指示灯亮，则继续判断指示灯颜色；若电源指示灯仍不亮，可联系 H3C 400-810-0504 解决。

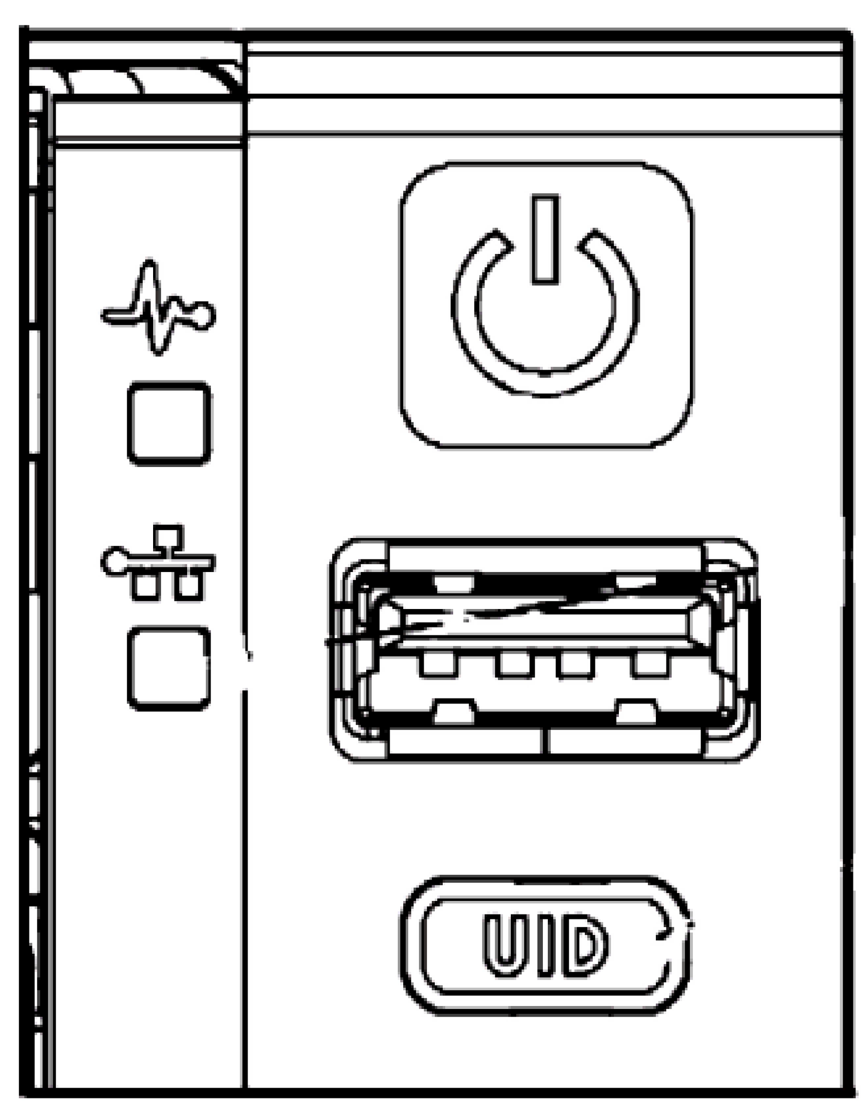


图 9-75　系统电源指示灯

(3) 系统电源指示灯是否为琥珀色

系统电源若点亮且为琥珀色，说明服务器处于待机状态，此时服务器可能没有开机，也可能由于电源问题、处理器故障或服务器硬件温度过高造成服务器未启动。

(4) 按下服务器电源后电源指示灯是否变绿

电源指示灯为琥珀色可能是服务器处于待机状态，对系统电源指示灯为琥珀色的服务器

按下电源，服务器若正常启动则系统电源指示灯会变绿。当然，也可能服务器由于故障继续保持琥珀色。

(5) 检查 SID 中 PROCS、OVER TEMP 与 PS1/PS2 指示灯状态

图 9-76 所示为 SID 指示灯。

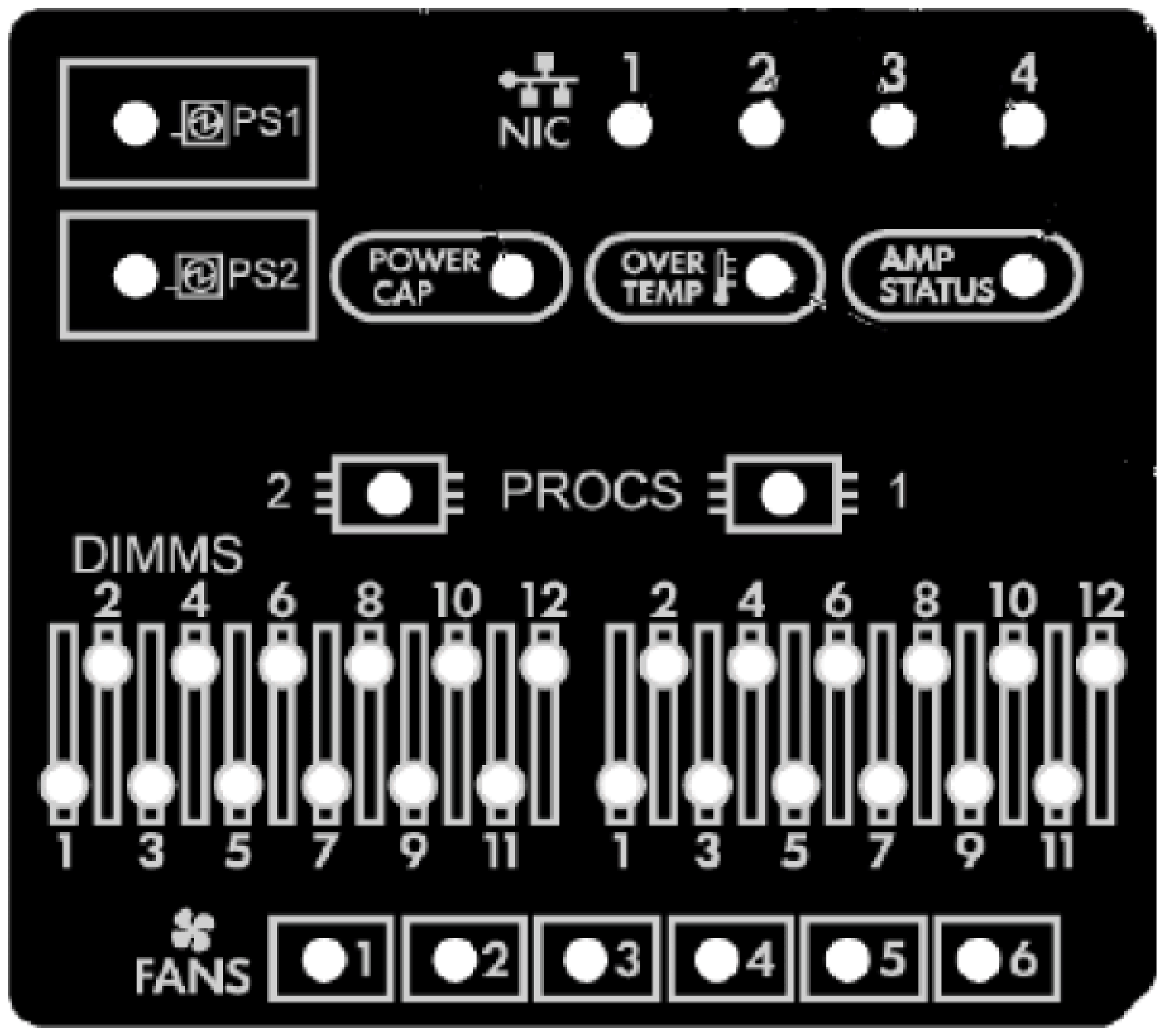


图 9-76　SID 指示灯

运行状况指示灯点亮，则一定为红色，并且可能存在以下 3 种故障。

① PROCS 指示灯若为琥珀色，则可能存在以下一种或多种情况，可联系 H3C 400-810-0504 解决。

(a) 插槽 X 中的处理器出现故障。

(b) 处理器 X 未安装在插槽中。

(c) 不支持处理器 X。

(d) POST 期间 ROM 检测到处理器有故障。

② OVER TEMP 指示灯若为琥珀色，服务器已检测到硬件临界温度，请保证服务器环境温度不要过高。

③ PS1/PS2 指示灯若为琥珀色，可能存在以下一种或多种情况。

(a) 只安装了一个电源，并且该电源处于待机模式。

(b) 电源故障，可联系 H3C 400-810-0504 解决。

(c) 主板故障，可联系 H3C 400-810-0504 解决。

(6) 查看运行状态指示灯是否为绿色

服务器电源指示灯为绿色的情况下，查看运行状态指示灯是否为绿色。

(7) 检查服务器是否运行正常

若服务器的运行状况指示灯为绿，说明服务器未发现故障，此时测试服务器业务是否运行正常，如有异常可联系 H3C 400-810-0504 解决。

(8) 查看运行状态指示灯是否为琥珀色

如果运行状况指示灯不是绿色，要判断运行状况指示灯是红色还是琥珀色来判断故障。

(9) 检查 SID 中 PROCS、DIMM、OVER TEMP、FANS 与 PS1/PS2 指示灯状态

运行状况指示灯如果为琥珀色，存在以下 5 种故障可能，可联系 H3C 400-810-0504 解决。

① PROCS 指示灯若为琥珀色，表示插槽 X 中的处理器处于故障前的状态。

② DIMM 指示灯若为琥珀色，表示插槽 X 中的 DIMM 处于故障前的状态。

③ OVER TEMP 指示灯若为琥珀色，表示运行状况驱动程序已检测到警戒温度。

④ FANS 指示灯若为琥珀色，表示一个风扇出现故障或已取下。

⑤ PS1/PS2 指示灯若为琥珀色，可能存在以下一种或多种情况。

(a) 安装了冗余电源，并且只有一个电源正常工作。

(b) 交流电源线未插入冗余电源上。

(c) 冗余电源故障。

(d) 在 POST 期间电源不匹配，或通过热插拔方式添加的电源不匹配。

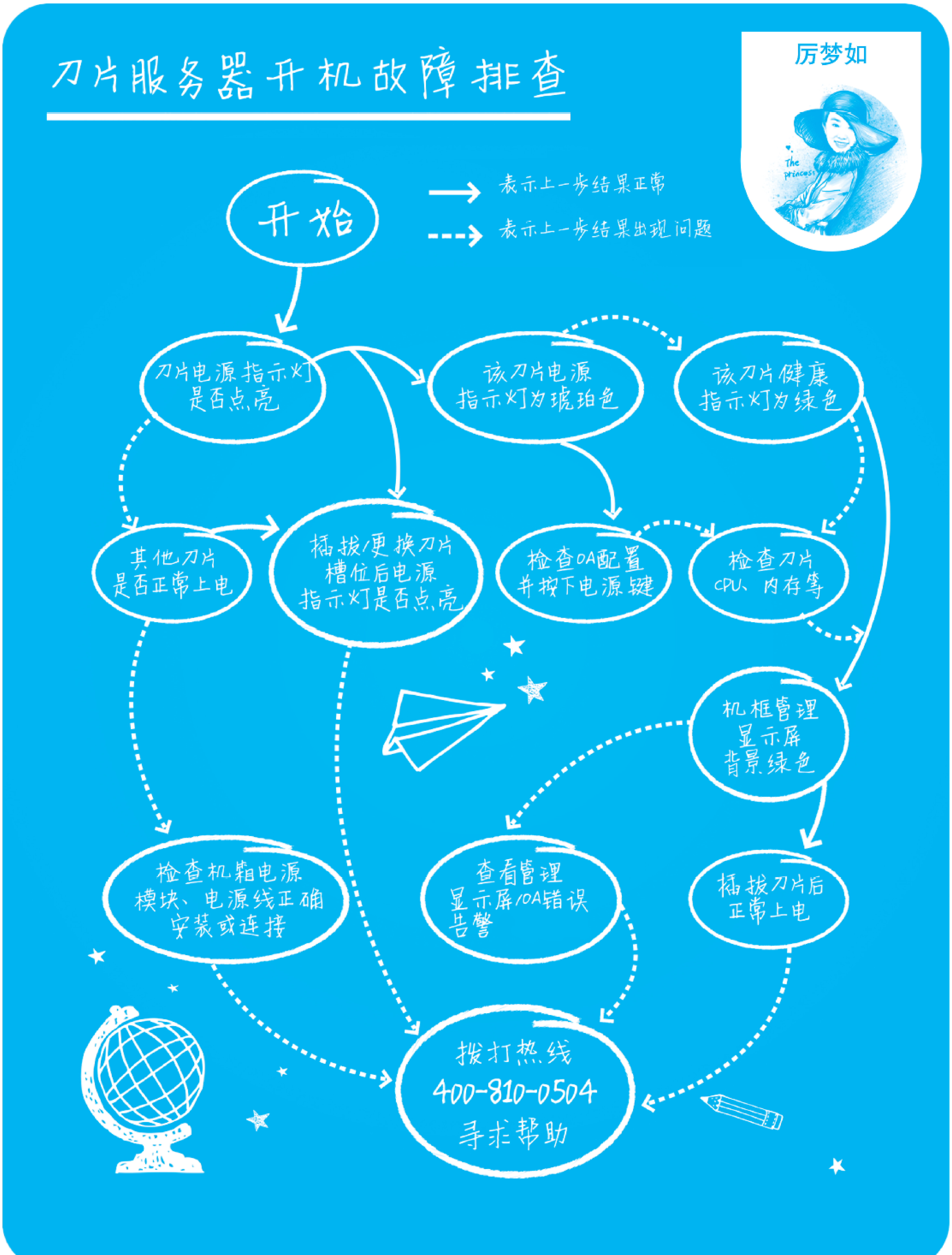
(10) 检查 SID 中 DIMM 与 FANS、PS1/PS2 及 PCI 转接卡指示灯状态

运行状况指示灯如果为红色，存在以下 3 种故障可能，可联系 H3C 400-810-0504 解决。

① DIMM 指示灯若为琥珀色，表示一个或多个 DIMM 出现故障。

② FANS 指示灯若为琥珀色，表示两个或多个风扇出现故障或已取下。

③ PCI 扩展插卡上的 PCI 转接卡指示灯若为琥珀色，表示 PCI 转接卡笼未正确就位。


刀片服务器开机故障排查
厉梦如
开始
表示上一步结果正常
表示上一步结果出现问题
刀片电源指示灯是否点亮
该刀片电源指示灯为琥珀色
该刀片健康指示灯为绿色
其他刀片是否正常上电
插拔/更换刀片槽位后电源指示灯是否点亮
检查OA配置并按下电源键
检查刀片CPU、内存等
机框管理显示屏背景绿色
检查机箱电源模块、电源线正确安装或连接
查看管理显示屏/OA错误告警
插拔刀片后正常上电
拨打热线
400-810-0504
寻求帮助

1. 开始

FlexServer B390/B590 刀片服务器出现开机故障时，可以通过服务器前面板的 LED 指示灯、机框上的管理显示屏和 OA 管理模块显示信息判断服务器无法正常开机的原因。

FlexServer 前面板主要包括健康指示灯①、系统电源指示灯②、UID 指示灯③和 FlexibleLOM LED 指示灯④。如图 9-77、图 9-78 所示分别是半高和全高刀片服务器。

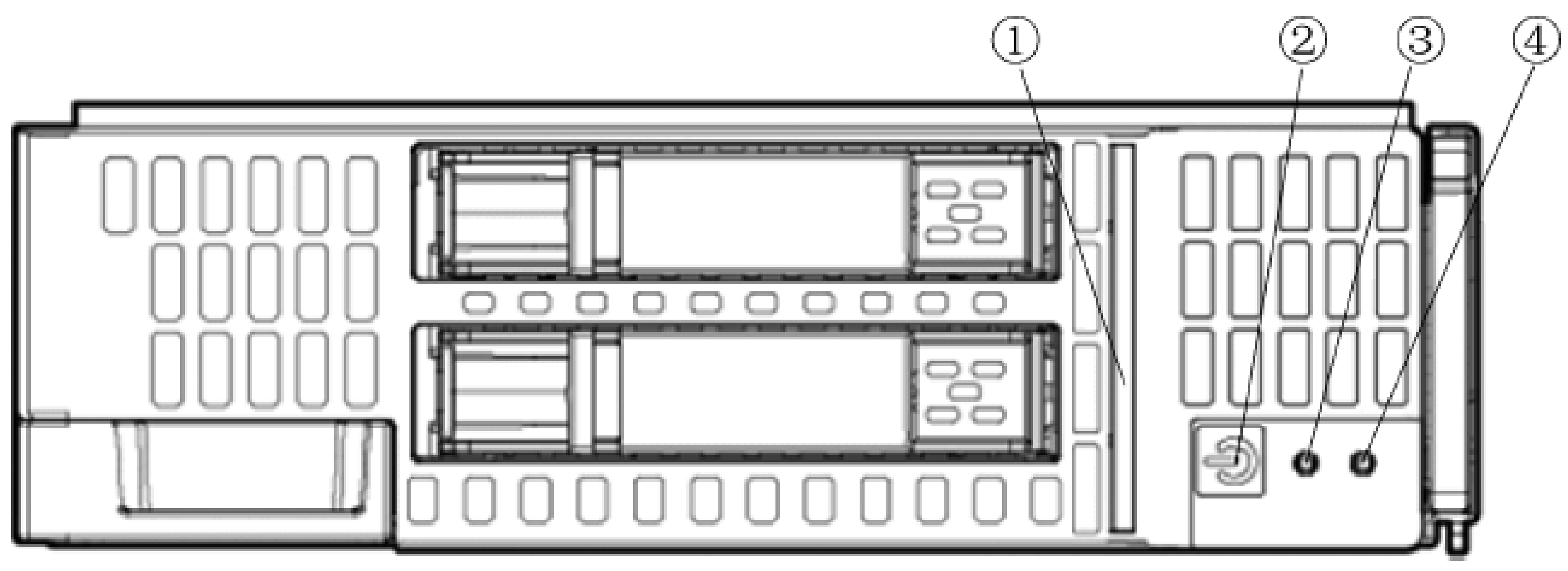


图 9-77 半高服务器前面板指示灯

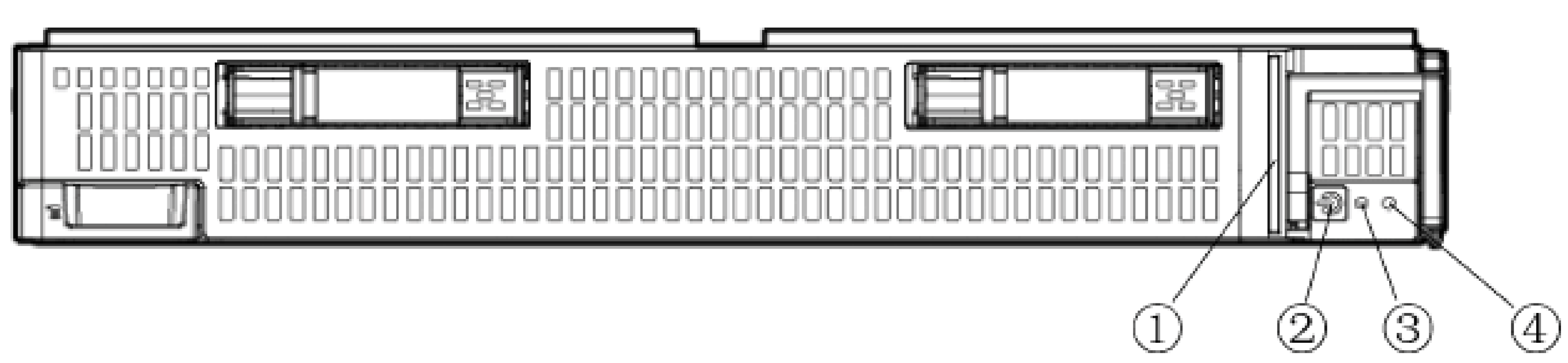


图 9-78 全高服务器前面板指示灯

机框管理显示屏位于机箱前面的中下方，可以查看整个机箱的健康和操作状态等信息，如图 9-79 所示。



图 9-79 机框管理显示屏

OA(Onboard Administrator)是机箱的管理单元，如图 9-80 所示，它可以提供基于 GUI 的管理界面，用户可以通过浏览器软件方便的管理机箱中的主要部件：刀片、电源、风扇和一

些扩展连接模块。如图 9-81 所示是 OA 管理登录界面。

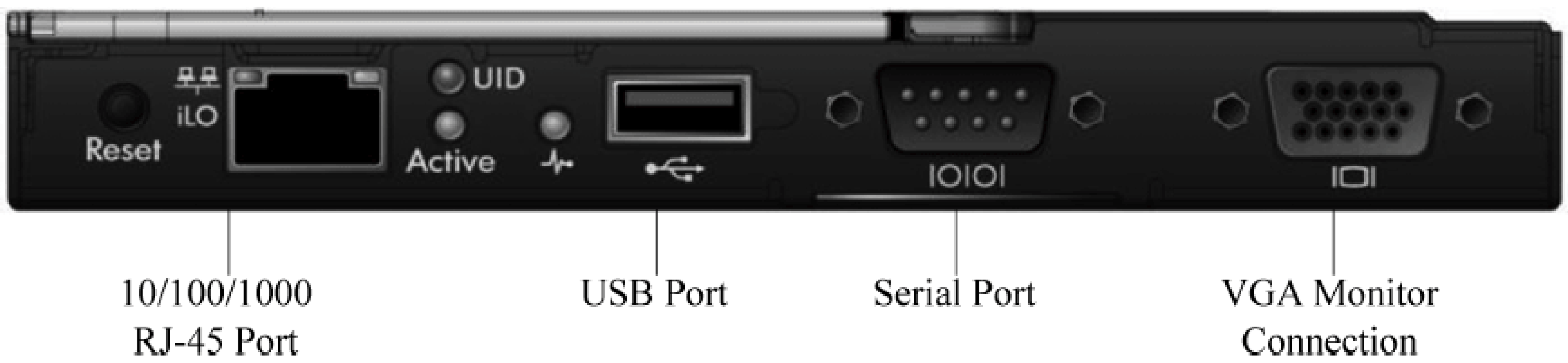


图 9-80　OA 管理模块

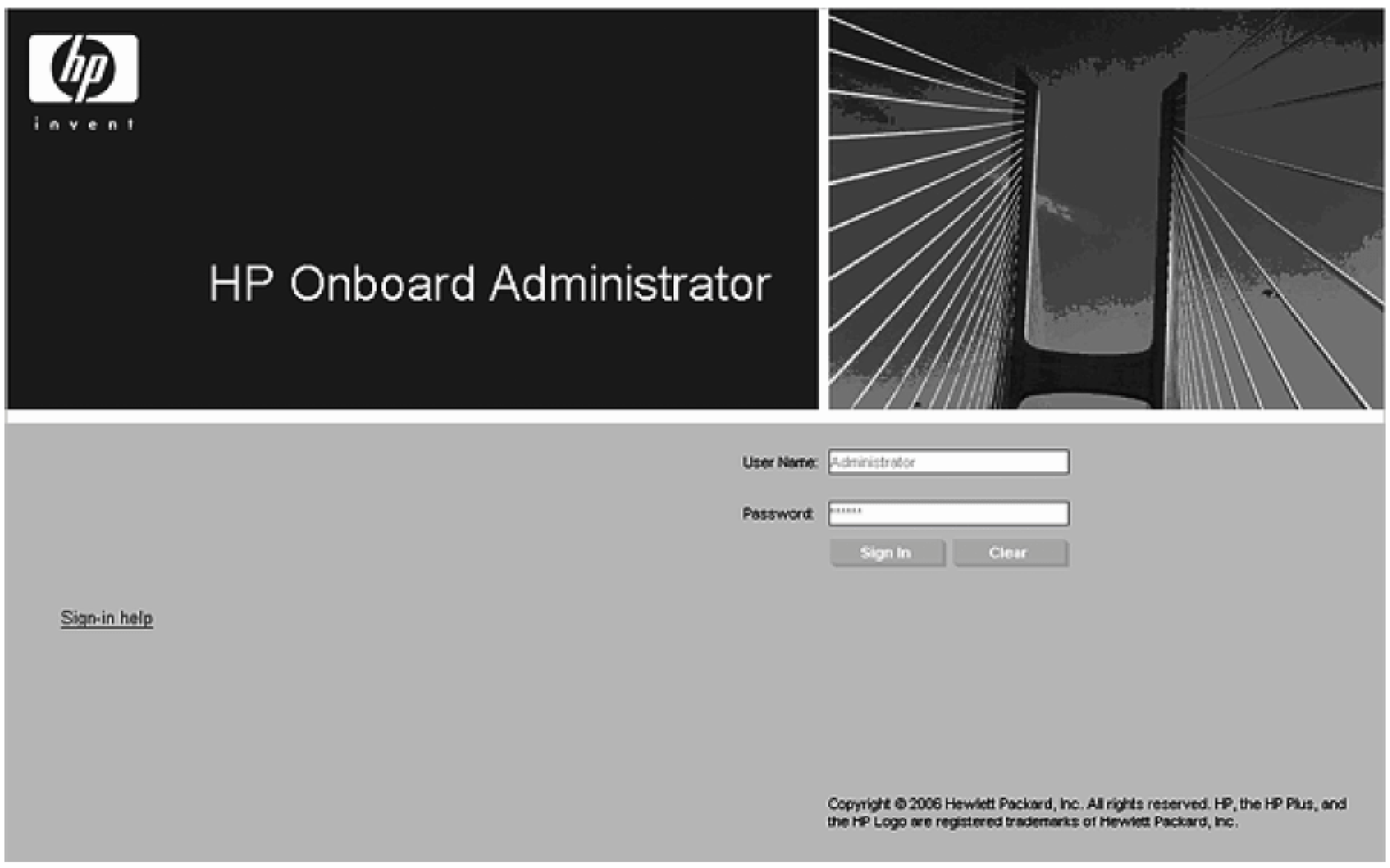


图 9-81　OA 管理登录界面

根据指示灯的不同状态以及不同组合，可初步判断以下 4 类服务器硬件故障类型。

① 刀片服务器未正确安装/配置。

② 机箱电源模块未正确安装/故障/缺失。

③ OA 模块未正确配置(如供电限额、电源冗余模式)。

④ 刀片服务器本身硬件未正确安装/配置(如内存)。

因此服务器硬件故障的排查思路如下。

① 若所有服务器插入机框后电源 LED 指示灯均不亮，查看机箱电源模块是否插牢，替换电源线排除电源线故障。

② 该刀片服务器插入机框后电源 LED 指示灯均不亮，检查刀片服务器的安装和配置。

③ 检查 OA 管理配置。

④ 登录 OA/管理显示屏，检查是否存在供电不足(需更改机箱电源配置或增加电源模块)、查看是否有其他告警并根据告警提示的解决方案处理。

2. 流程图相关操作说明

(1) 刀片电源指示灯是否点亮

查看服务器电源指示灯，如图 9-82 编号②所示。如果电源指示灯亮，则继续判断指示灯颜色；若电源指示灯仍不亮，则开始排查刀片无法供电原因。

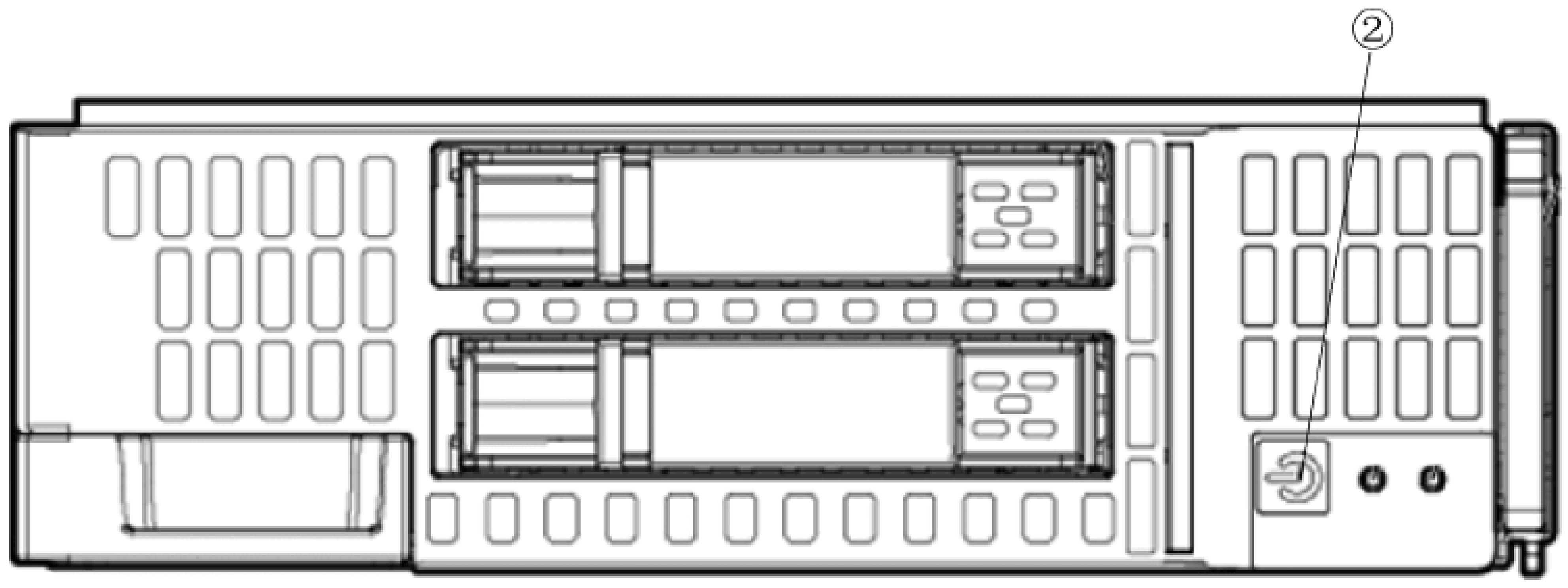


图 9-82 检查电源指示灯

(2) 其他刀片是否正常上电

查看其他刀片服务器是否正常上电，如果上电正常，则问题定位在该刀片服务器本身(安装、配置或者硬件问题)；否则，则排查机框供电(电源线和电源模块是否存在问题、OA 上的配置是否正确)。

若如图 9-83 所示服务器的电源指示灯②和健康指示灯①都是绿色，说明服务器未发现故障，同时也可以正常开机、启动，说明刀片服务器硬件正常。

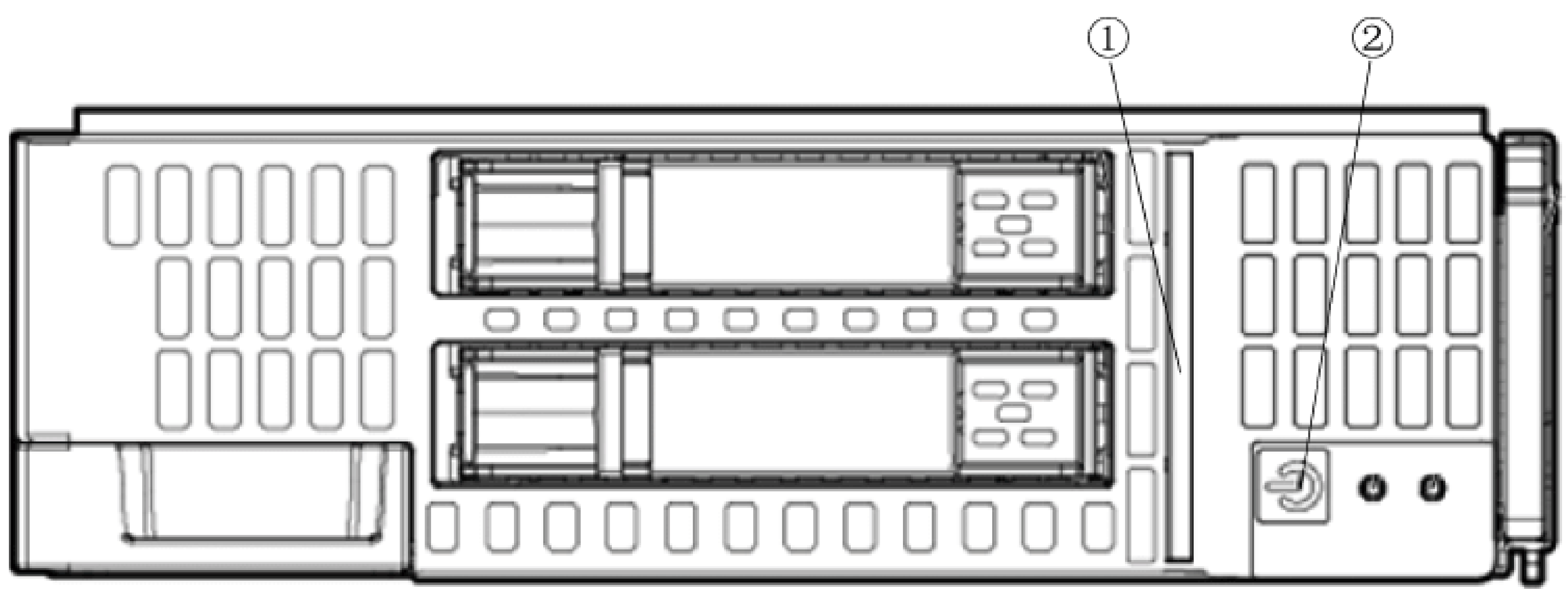


图 9-83 刀片服务器前面板指示灯

(3) 检查机箱电源模块、电源线正确安装或连接

按照如下步骤检查机框电源线和电源模块。

① 电源线是否松动。

② 电源线是否故障，寻找其他电源线进行替换验证，确认电源线正常。

③ 重新安装电源模块：电源模块安装没有正确就位，会导致服务器无法正常开机。因此先断开电源线，然后拔出并重新安装电源模块。

如果以上步骤执行完毕后系统电源指示灯亮，则继续判断指示灯颜色；若电源指示灯仍不亮，可联系 H3C 400-810-0504 解决。

(4) 插拔/更换刀片槽位后电源指示灯是否点亮

插拔刀片服务器是为了确认服务器安装正确，检查步骤如下。

① 确认问题刀片服务器。

② 按照如图 9-84 所示拆卸刀片服务器。

③ 将刀片服务器重新安装进机箱。

如果本步骤执行完毕后系统电源指示灯亮，则继续判断指示灯颜色；若电源指示灯仍不亮，则对刀片服务器进行更换槽位，同时联系 H3C 400-810-0504 解决。

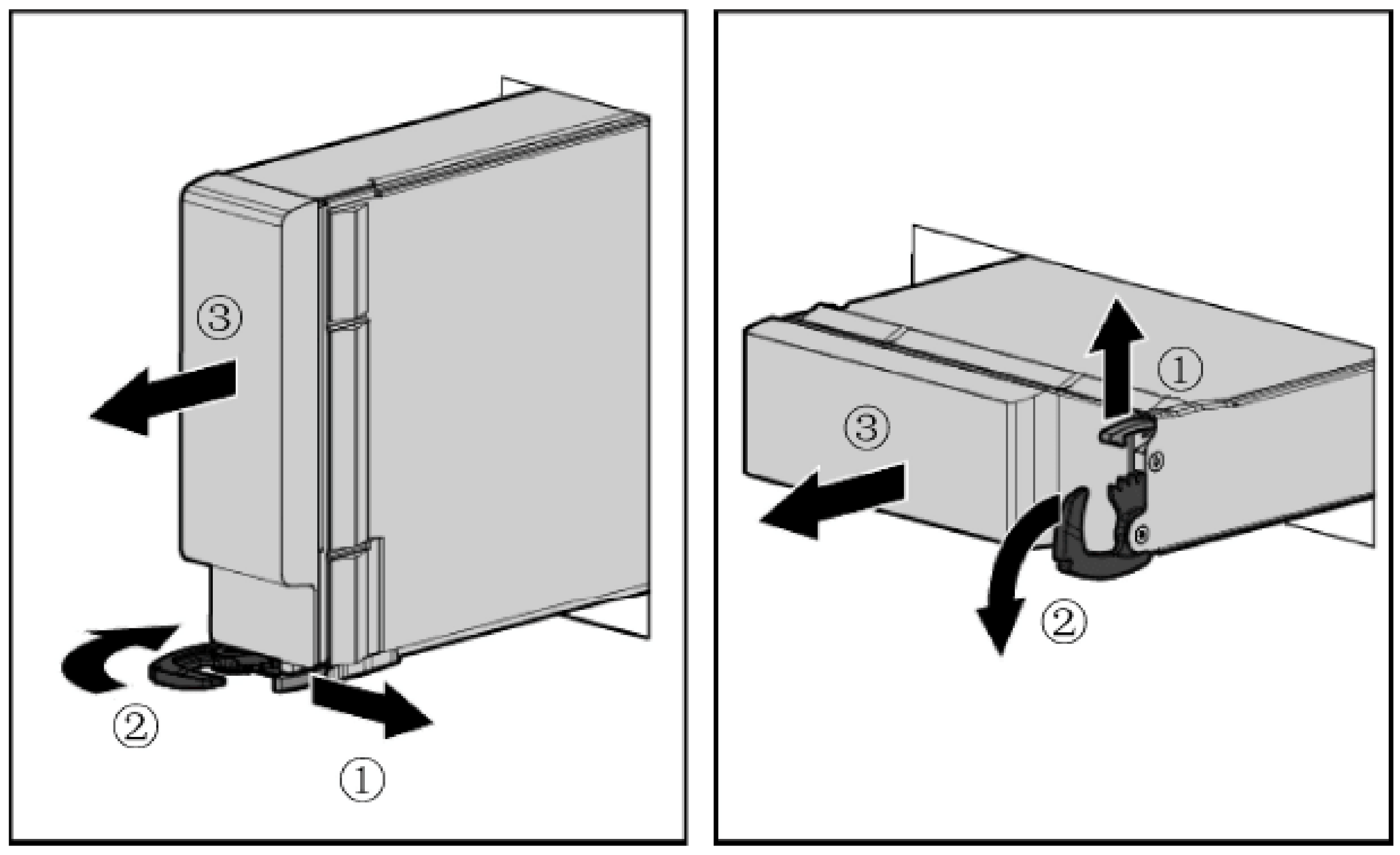


图 9-84　拔出刀片服务器

更换刀片服务器所在槽位是为了确认机箱中间板供电良好，步骤如下。

① 确认问题刀片服务器。

② 按照如图 9-84 所示拆卸刀片服务器安装到其他槽位。

说明：

(a) 更换测试的槽位，优先选择空余槽位。如果没有空槽位，在不影响客户业务的前提下，将其中一台供电正常的刀片服务器正常关机，拆卸并放在平坦的工作面上。在检测完成后再将服务器回归原来槽位。

(b) 为减少设备表面过热而造成人身伤害的危险，请在驱动器和内部系统组件散热后再触摸它们。为防止电子器件受损，请在开始任何安装过程之前，将服务器刀片正确接地。接地不当可能会释放静电。

(5) 该刀片电源指示灯为琥珀色

查看服务器电源指示灯，如图 9-85 编号②所示。系统电源指示灯若点亮且为琥珀色，说明服务器处于待机状态，此时服务器可能有如下情况。

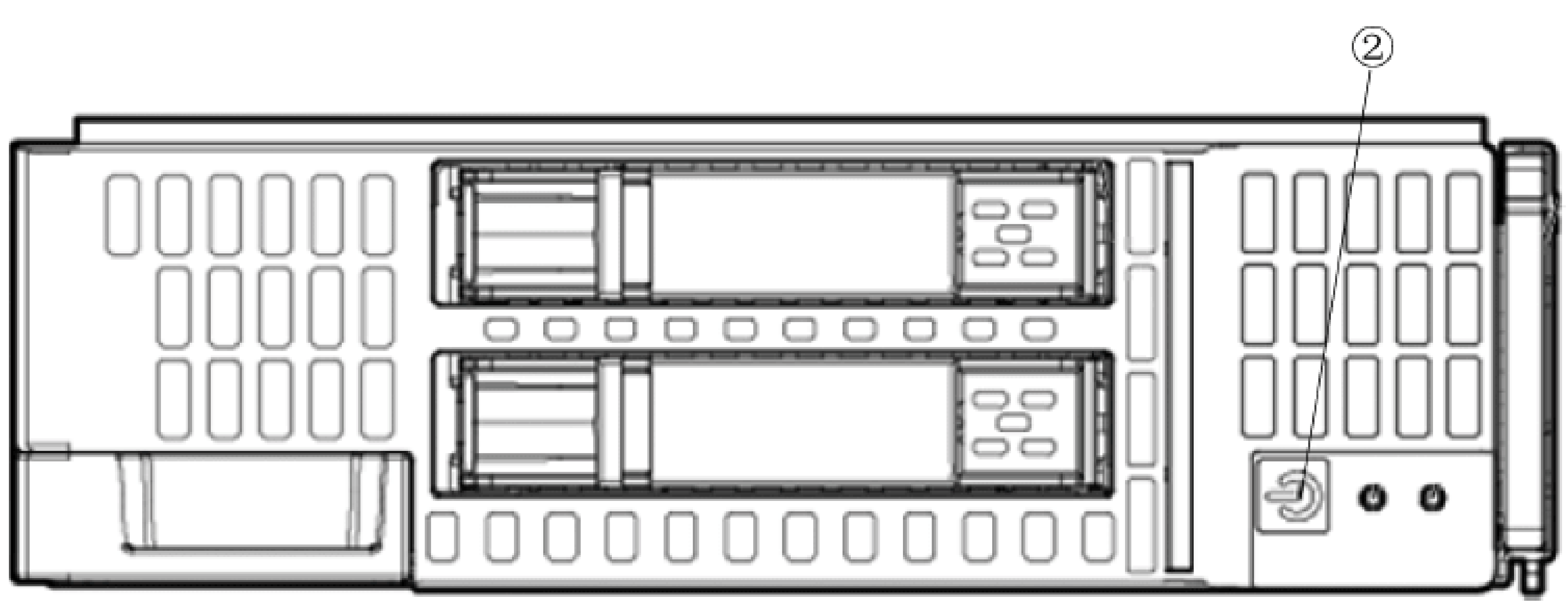


图 9-85　检查电源指示灯是否为琥珀色

① 服务器没有开机。

(a) 服务器首次安装，没有按开机的电源键。

(b) 机框之前重启过，在 OA 上配置不默认启动。

② 电源供电不足(OA 配置电源冗余模式不合理)造成服务器未启动。

③ 内存问题造成服务器未启动。

④ 其他问题导致(根据管理显示屏/OA 提示进一步分析处理)。

（6）检查 OA 配置并按下电源键

如图 9-86 编号②所示，按下电源键将服务器开机。

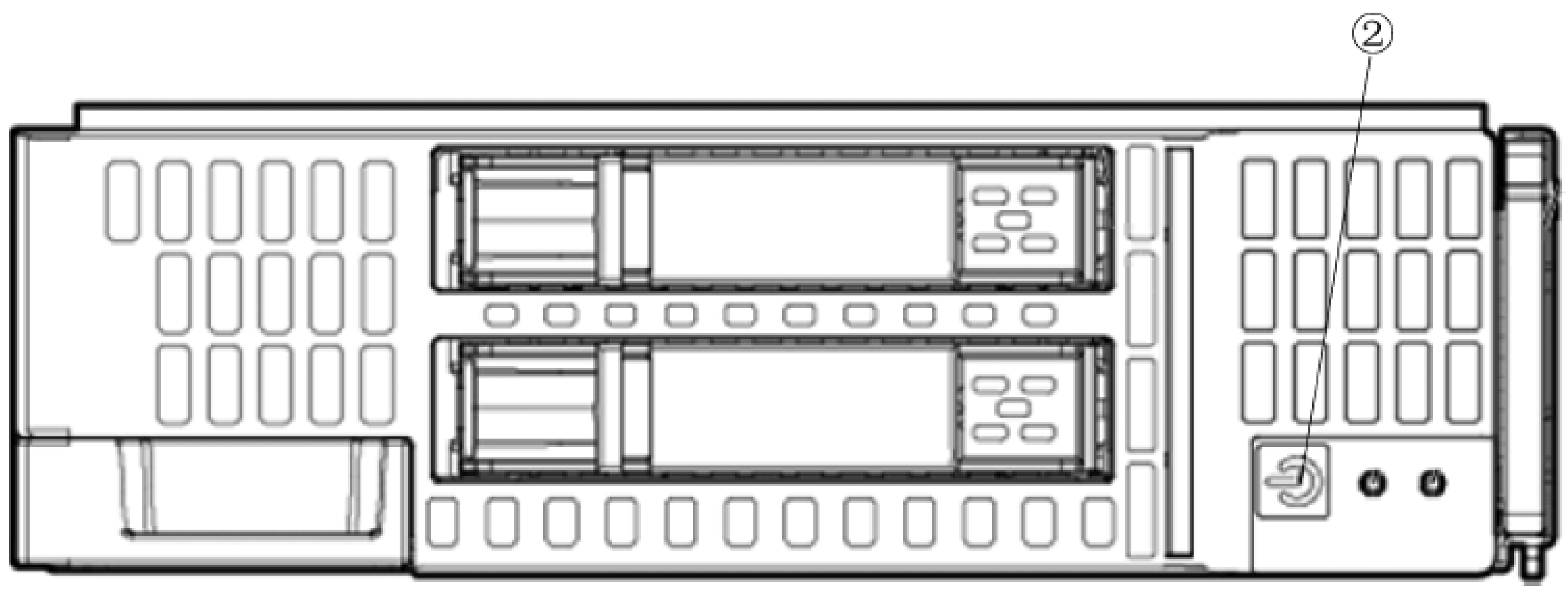


图 9-86 按下电源键

如果服务器能仍无法开机，则需要登录 OA 查看是否有供电不足的情况，如图 9-87 所示。如果确实存在供电不足情况，解决方法是提高设置的供电上限额度、增加电源模块（推荐）或者修改电源冗余模式降低冗余性（如 N+N 冗余改成无冗余）。

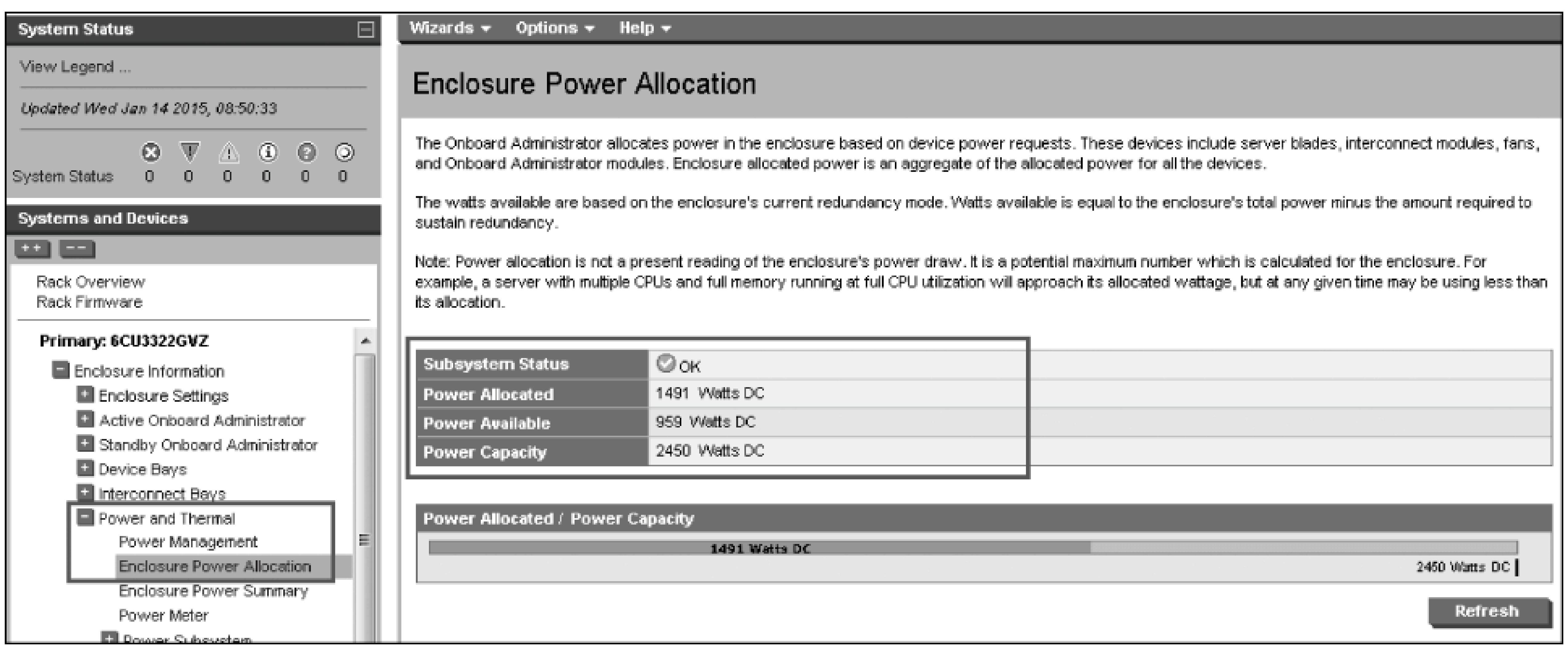


图 9-87 机箱电源供电统计

机框功率限额设置过低，会导致供电不足，如图 9-88 所示。

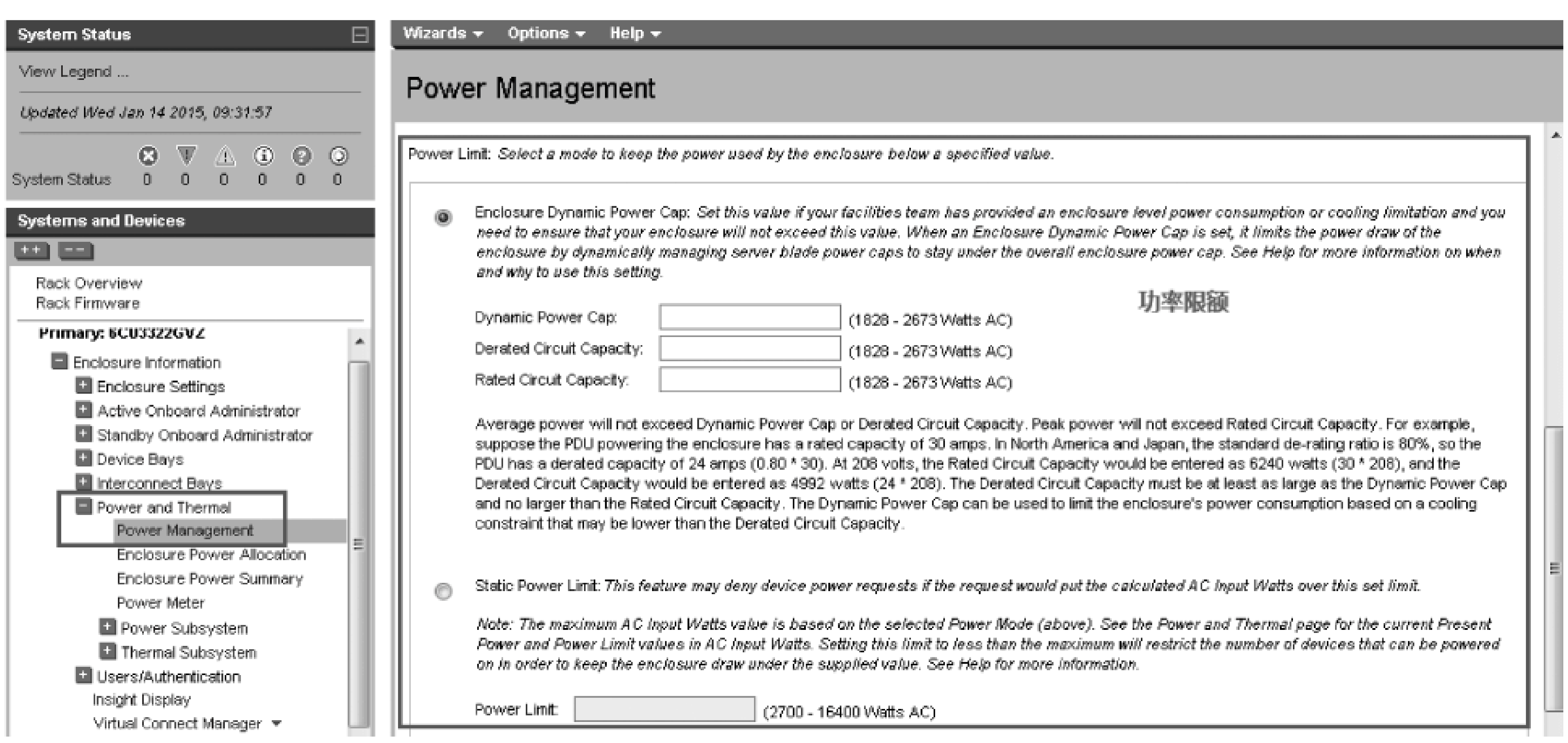


图 9-88 机箱供电功率限额设置

电源冗余模式有 3 种，如图 9-89 所示。

① No Redundant(无冗余)。

② Power Redundant(N+1)。

③ AC Redundant (N+N)。

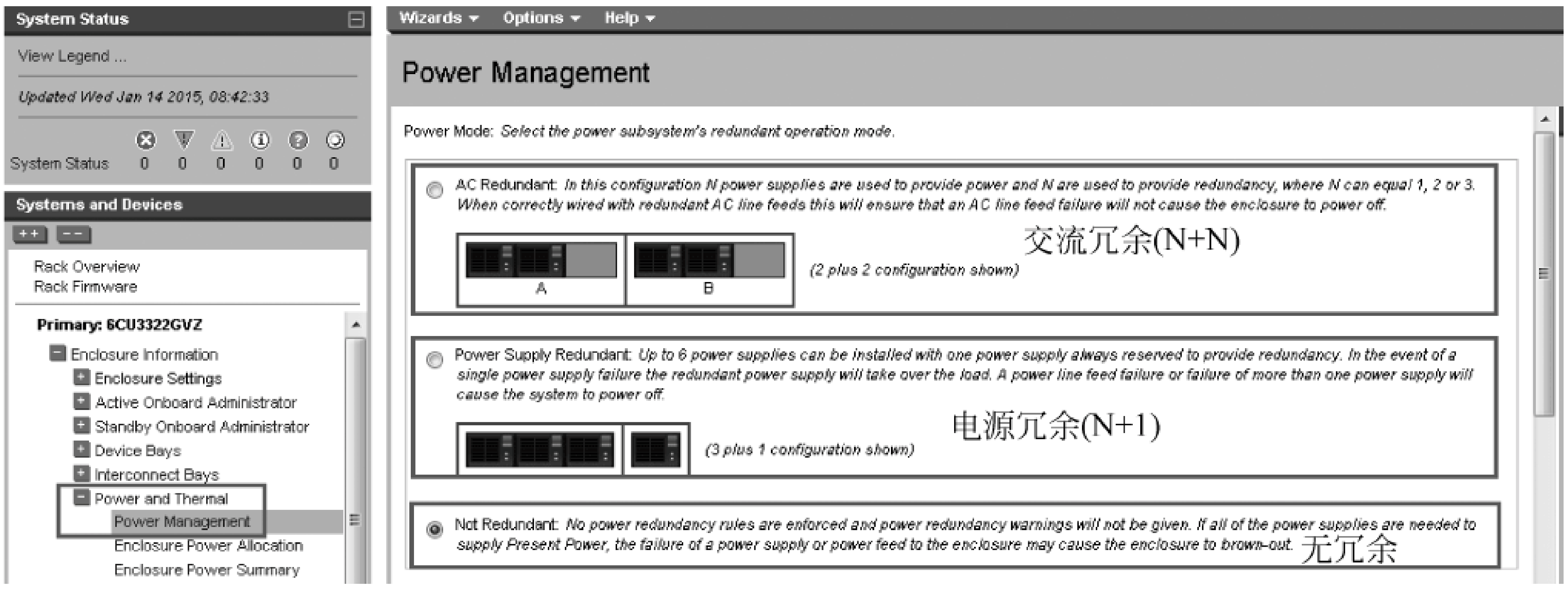


图 9-89　机箱电源冗余模式

机框重启后服务器是否自动开机可以在 OA 界面上设置，即如果发现服务器不是开机状态，原因也可能是由于之前机框重启过且 OA 界面设置了服务器不会自动启动，如图 9-90 所示。

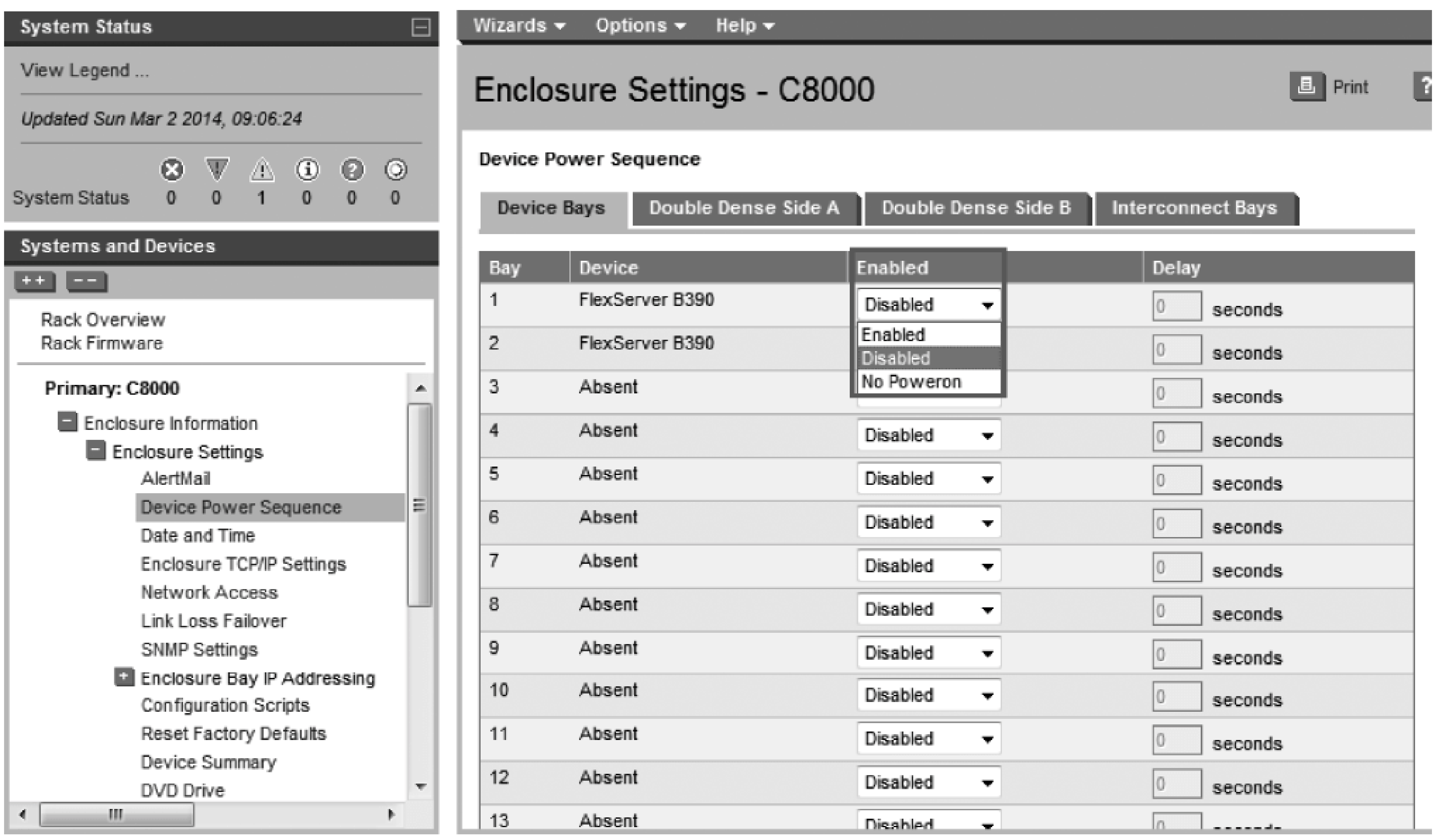


图 9-90　机箱设备电源启动顺序设置

(7) 检查刀片 CPU、内存等

刀片服务器 CPU 或内存缺失、故障或者安装不正确都可能导致服务器启动异常。登录该刀片服务器的 iLO 界面或者将显示器直连服务器，在服务器重启过程中查看自检过程是否有 CPU、内存等告警，根据相应的提示是内存故障、缺失还是安装错误进行相应处理。

如果提示硬件故障，请联系 H3C 400-810-0504 处理。

例如：如图 9-91 所示，在服务器启动过程中发现有“207-DIMM Error：Processor 1，DIMM 4

has receved an uncorrectable error”的告警，即 CPU1 对应的 4 号内存插槽上的内存硬件报错。

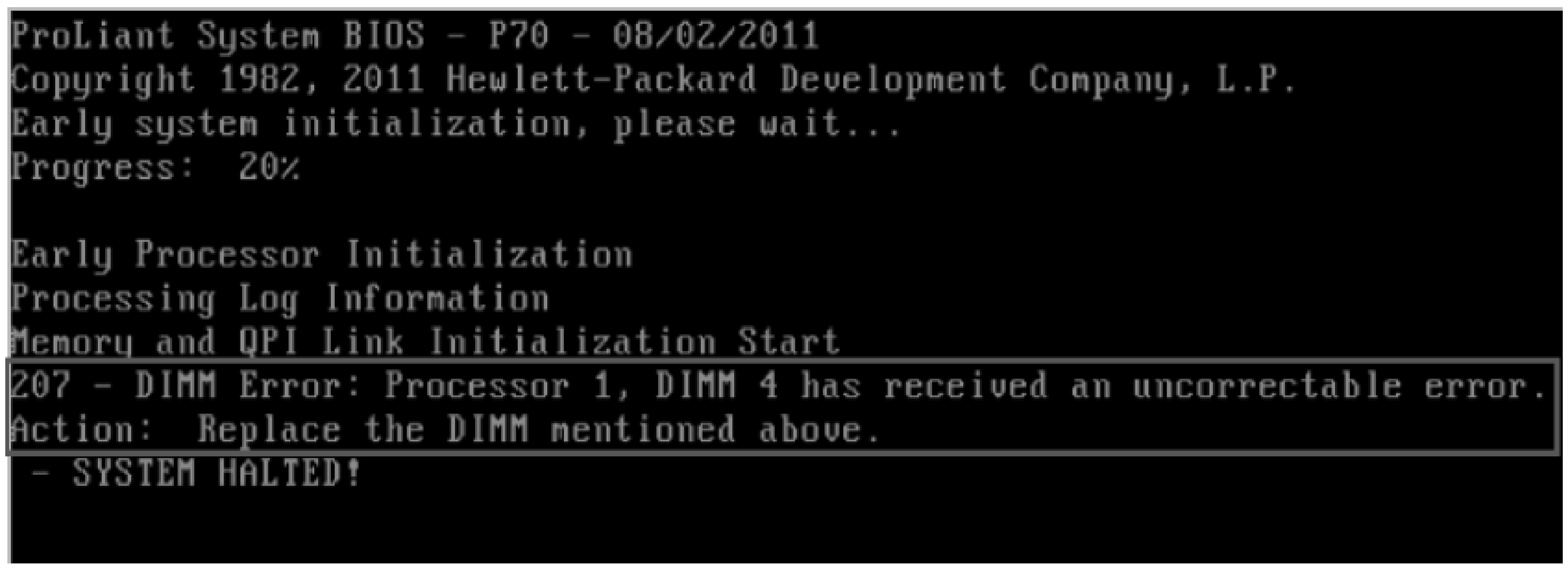


图 9-91　CPU1 对应的 4 号内存插槽的内存硬件报错

（8）该刀片健康指示灯为绿色

查看服务器健康指示灯，如图 9-92 编号①所示。如果是绿色说明正常，如果闪红色或者琥珀色说明可能是 CPU、内存等问题。

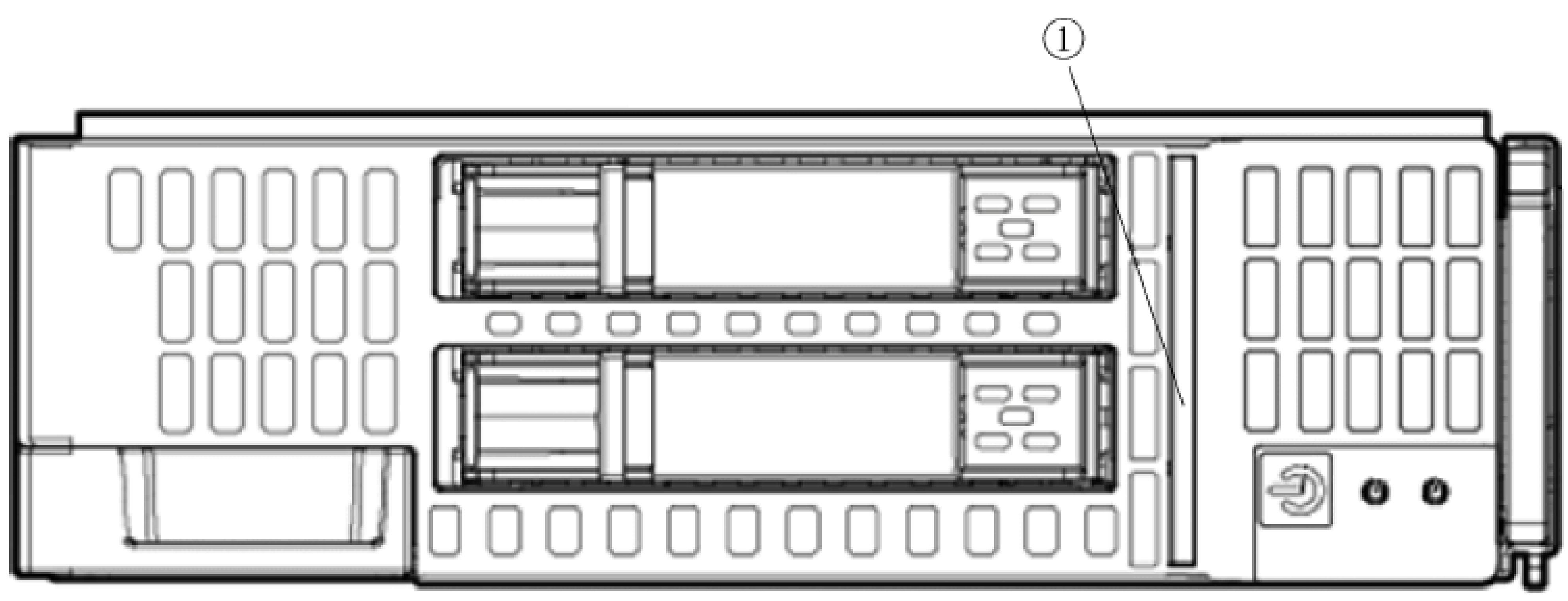


图 9-92　检查键康指示灯

（9）机框管理显示屏背景绿色

查看机框管理显示屏的背景颜色，即查看整个机箱的健康状态等信息，如图 9-93、图 9-94 所示。

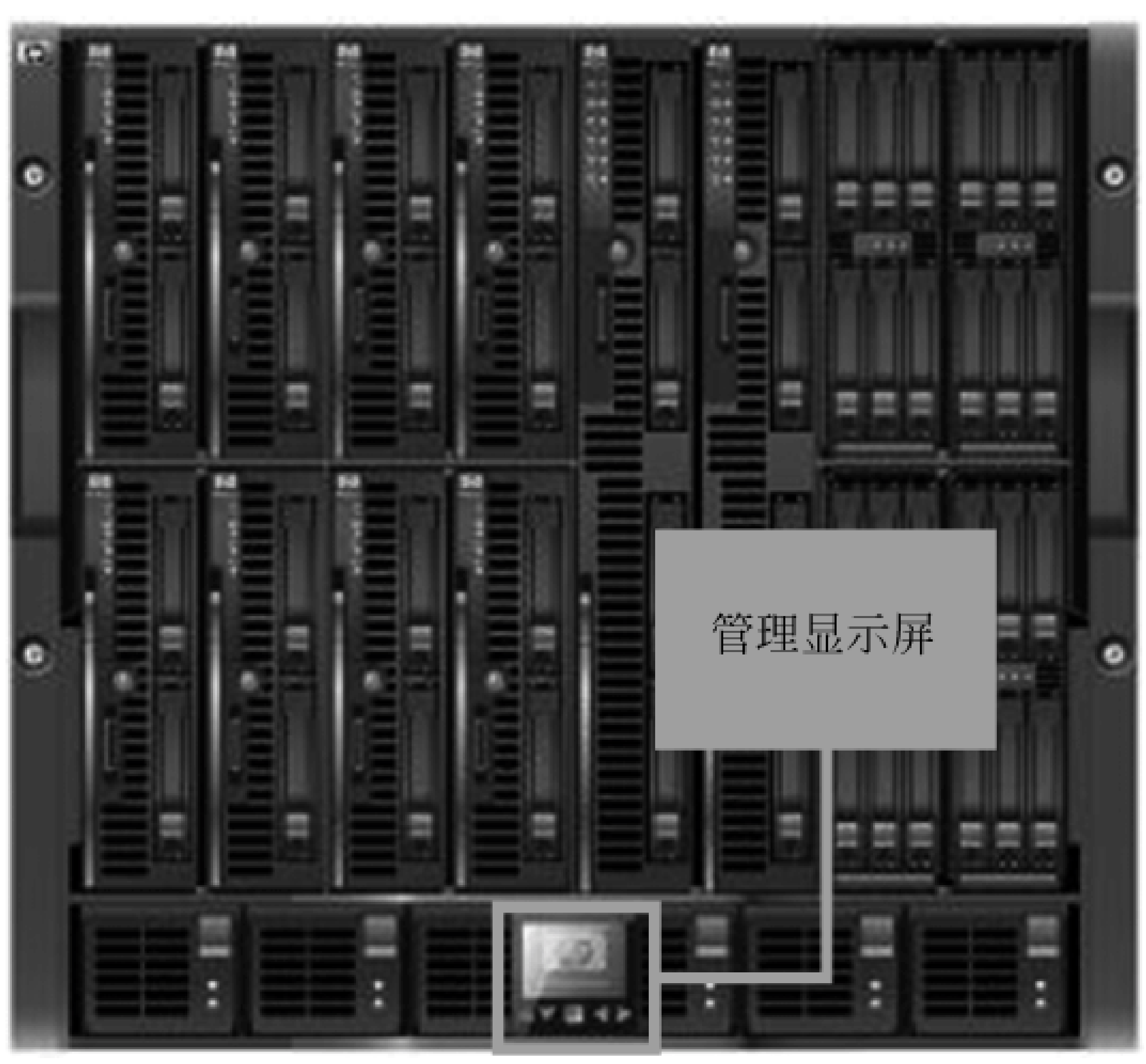


图 9-93　机框管理显示屏



图 9-94　机框管理显示屏示意图

不同的状态下颜色定义如下。

① 蓝色：机器没有错误且 UID 被设为 ON 的状态。

② 绿色：机器没有任何错误或警告，2 分钟后变暗。

③ 橘黄色：机器出现错误或警告。

(10) 插拔刀片后正常上电

插拔刀片服务器是为了确认服务器安装正确，如图 9-84 所示，检查步骤如下。

① 确认问题刀片服务器所在槽位。

② 按照下图拆卸刀片服务器。

③ 将刀片服务器重新安装进机箱。

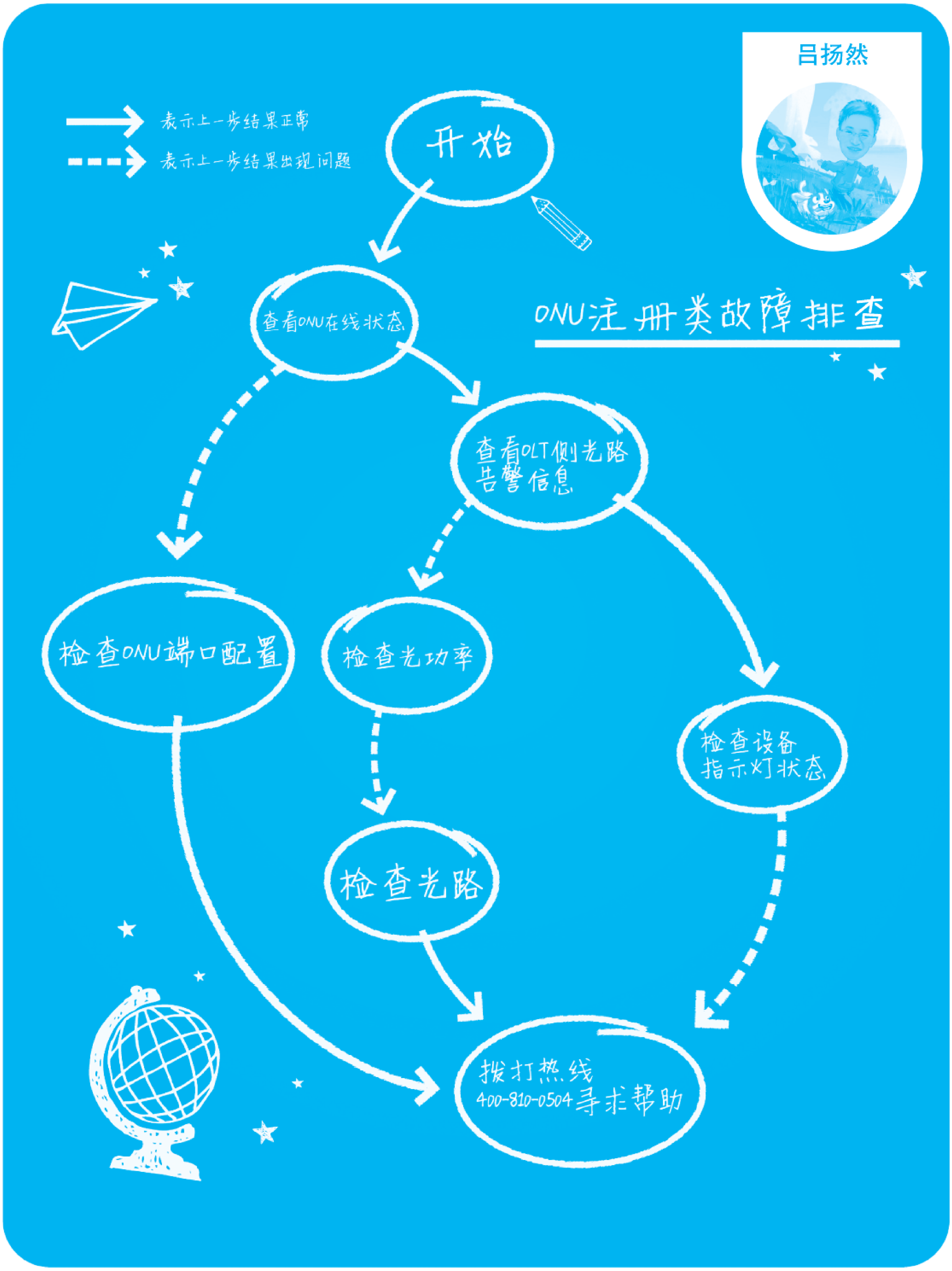
如果本步骤执行完毕后刀片服务器开机仍不正常，即可联系 H3C 400-810-0504 解决。

(11) 查看管理显示屏/OA 错误告警并按照解决提示信息操作

通过管理显示屏或者 Web 登录 OA 管理界面(推荐)查看是否有相应告警信息，如风扇散热告警等，根据提示的解决方法信息处理。如果无法解决，即可联系 H3C 400-810-0504 处理。

10

EPON_EoC产品


吕扬然
表示上一步结果正常
表示上一步结果出现问题
开始
ONU注册类故障排查
查看ONU在线状态
查看OLT侧光路告警信息
检查ONU端口配置
检查光功率
检查设备指示灯状态
检查光路
拨打热线
400-810-0504寻求帮助

1. 开始

EPON 系统是由三部分组成，分别为 OLT、ODN 以及 ONU，中间的光分配网不存在有源设备，在很大程度上降低了设备的维护成本，但是由于光纤的特殊性，很容易引入损耗问题。所以，定位故障的思路是：先查配置、再查光路、最后再查看是否是设备硬件问题。

2. 流程图相关操作说明

(1) 查看 ONU 在线状态

查看对应 ONU 的当前状态。

① 若当前 ONU 状态显示为 Up，说明 ONU 已经绑定，属于正常状态。

② 若当前 ONU 状态显示为 Silent，说明 ONU 处于静默状态，未在对应的 ONU 端口绑定 MAC。

③ 若当前 ONU 状态显示为 Offline，说明 ONU 已绑定 MAC，但由于绑错 MAC 地址或者其他原因导致 ONU 无法 Up。

④ 若当前 ONU 状态显示为 Down，说明 ONU 已绑定 MAC，但由于 ONU 端口被手工 Shutdown 或者其他原因导致 ONU 无法 Up。

命令：*display onuinfo slot slot-number*

例如：通过命令查看，确认当前 ONU 状态。

```
[H3C]display onuinfo slot 2
-----------------------------------Olt2/0/1--------------------------------
ONU Mac Address   LLID  Dist(M)   Port         Board/Ver   Sft/Epm   State    Aging
000f-e2b9-cdf7     2     <1       Onu2/0/1:1   ET716/B     105/100   Up       N/A
000f-e26f-a230     1      2       Onu2/0/1:2   ET254-L/B   118/100   Up       N/A
0cda-41e3-5468     3     <1       Onu2/0/1:3   ET254-L/B   111/100   Down     N/A
0023-89b9-34a1     0     N/A      Onu2/0/1:4   N/A         N/A       Offline  N/A
000f-e2b8-2638     0     N/A      N/A          N/A         N/A       Silent   272s
```

(2) 查看 ONU 端口配置

查看对应 ONU 端口视图下 OLT 下发给 ONU 的配置。

命令：*display this*

例如：通过命令查看，确认已绑定了正确的 ONU MAC 地址。

```
[H3C-Onu2/0/1:1] display this
#
interface onu2/0/1:1            //进入 ONU 端口视图
bind onuid 000f-e26f-a230       //绑定 ONU 的 MAC 地址
#
return
```

(3) 查看 OLT 侧光路告警信息

查看 OLT 上的 trapbuffer 是否存在大量的 FER(帧误码率)、BER(比特错误率)或者 OAM 告警。

命令：*display trapbuffer*

例如：通过命令查看，可以确认现网中是否存在大量的光路告警信息。

```
<H3C> display trapbuffer
Aug 20 13:43:38 2012 S75E EPON/1/TRAP_FER:
  Trap 1.3.6.1.4.1.2011.10.2.42.1.8.0.2(h3cEponPortAlarmFerTrap):A FER alarm trap has been
detected,                                //表示发现一个 FER 告警信息
  interface index is 201327022,
  entry index is 201327022,
  interface description is Onu2/0/1:1,          //表示接口描述
# Aug 20 18:40:55 2012 S75E EPON/1/TRAP_BER:
  Trap 1.3.6.1.4.1.2011.10.2.42.1.8.0.1(h3cEponPortAlarmBerTrap): A BER alarm trap has been
detected,                                //表示发现一个 BER 告警信息
  interface index is 134218102,
  entry index is 134218102,
  interface description is Onu2/0/1:2,          //表示接口描述
#Aug 20 15:34:41 2012 S75E EPON/1/TRAP_OAM_THRESHOLD:
  Trap 1.3.6.1.4.1.2011.10.2.42.3.1.7.0.1(h3cDot3OamThresholdEvent):An OAM threshold
event trap has been detected,              //表示发现一个 OAM 告警信息
  interface index is 268435822,
  OAM entry event index is 268435822,
```

(4) 查看光功率

查看 ONU 侧接收的光功率值。

使用光功率计测量 ONU 侧接收的光功率值，ONU 光功率参数如表 10-1 所示。

表 10-1　ONU 光功率参数

上下行波长	上行 1310nm，下行 1490nm
接收饱和光功率	－3dBm
接收灵敏度	－26.5dBm
发射光功率	＋4dBm～－1dBm

如果测量值在 ONU 的接收范围之外，都有可能导致注册不上。使用光功率计测量 ONU 的接收光功率值时，需注意测量的光纤位置，将接入 ONU PON 接口的光纤拔出接入到光功率计的指定端口进行测量。

如果 ONU 是 ET704-L-A/ET254-L-A/ET254-G-A，可以通过串口或者 Telnet 到 ONU 上，通过命令查看当前光功率信息。

命令：*display optics-power*

例如：通过命令查看，可以确认 ONU 接收光功率值是否正常。

```
<H3C>display optics-power              //显示 PON 接收/发送光功率信息
PON:
Receive :-16.78dBm                    //当前接收光功率信息
Transmit: 1.46dBm                     //当前发送光功率信息
```

(5) 检查光路

① 检查 ONU 侧尾纤接口是否为 SC/PC，若不是则需要更换尾纤。

② 使用专业清洁工具擦拭光纤链路上各接口的光纤截面，排查光纤端面污损引起。

③ 检查光纤链路各接口是否连接良好。

④ 检查光纤总长度是否小于 20km，可参考附近正常注册的 ONU 测距参数，如果超过

20km 需要调整光纤链路，以满足要求。

命令：*display onuinfo slot slot-number*

例如：通过命令查看，可以确认 ONU 到 OLT 的距离。

```
[H3C]display onuinfo slot 2
----------------------------------------Olt2/0/1----------------------------------------
ONU Mac Address   LLID  Dist(M)      Port      Board/Ver   Sft/Epm   State   Aging
000f-e2b9-cdf7      2       <1   Onu2/0/1:1     ET716/B   105/100    Up     N/A
000f-e26f-a230      1        2   Onu2/0/1:2   ET254-L/B   118/100    Up     N/A
```

⑤ 观察同一分光器下是否有其他 ONU 能够正常注册，如果在同一分光器下，没有正常注册的 ONU，则分光器或者该分光器主干线路存在问题；如果同一分光器下其他注册正常，需继续下一步排查。

⑥ 将故障 ONU 移至上一级分光器下测试是否正常。如果正常，说明该段尾纤存在问题，如果不正常，需继续下一步排查。

⑦ 替换主干光纤链路观察。

（6）检查设备指示灯状态

① 检查 ONU 的 Power 指示灯状态

检查 ONU 面板上的 Power 指示灯是否一直处于亮起状态，常亮则表示 ONU 供电正常；如果异常说明是电源输出问题或者设备故障。

检查电源问题如下。

（a）ONU 电源接口是否插紧，连接是否正常。

（b）插线板或插座是否已经通电，可接上其他电器设备验证。

（c）插线板或插座与 ONU 电源线接触是否良好。

（d）尝试更换一条电源线观察是否正常。

② 检查 ONU 的 Diag 指示灯状态

（a）检查 ONU 面板上的 Diag 指示灯，熄灭则表示设备工作在正常状态。

（b）如果亮一会儿就灭掉，说明是设备系统自检所致，属于正常情况。

（c）如果一直常亮或者闪烁，均表示设备故障，建议更换 ONU 观察。

③ 检查 ONU 的 PON 口指示灯状态

（a）检查 ONU 面板上的 PON 口指示灯是否一直处于亮起状态，常亮则表示 ONU 与 OLT 之间 PON 链路已经正常建立。

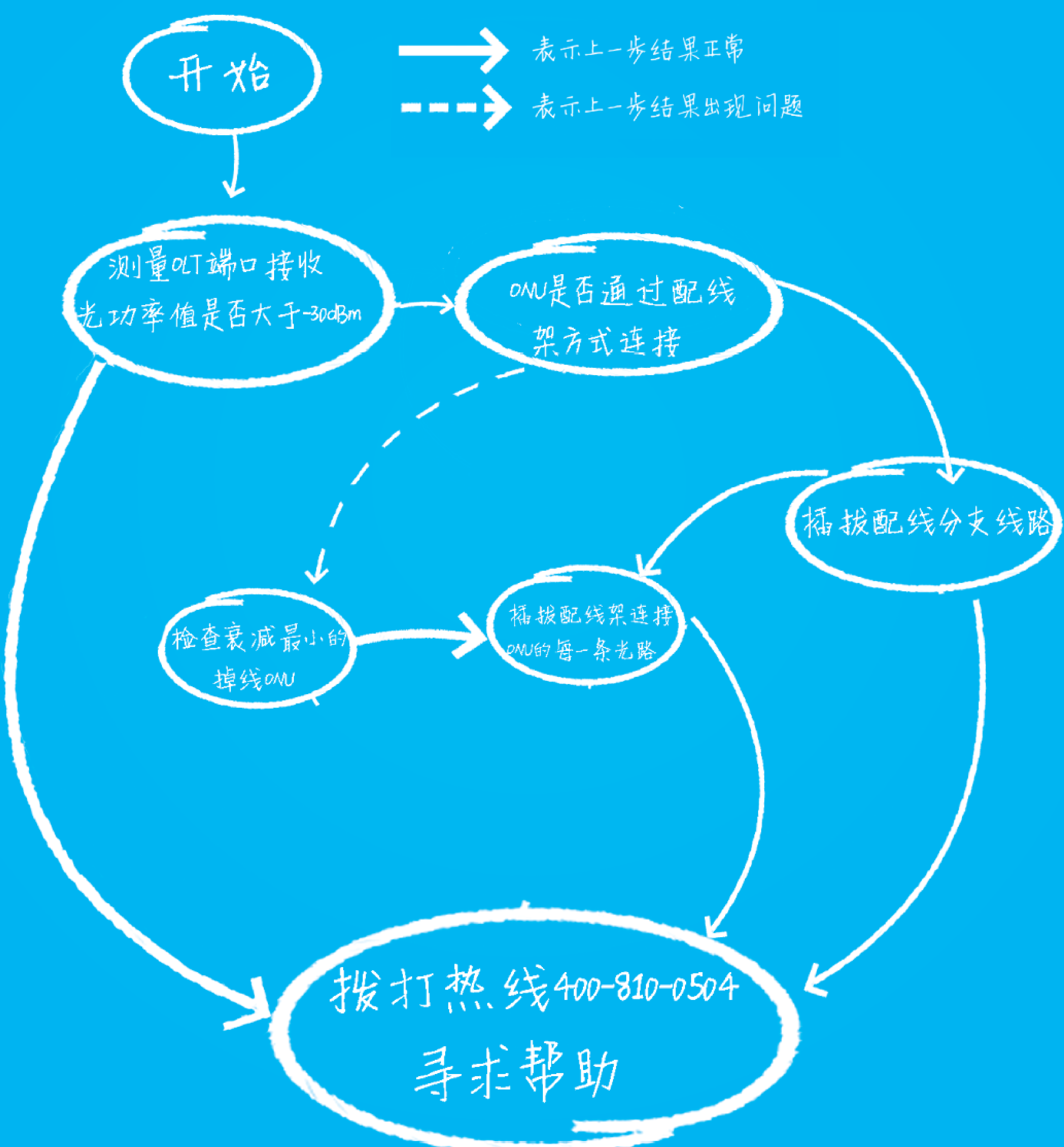
（b）如果一直处于闪烁状态，表示 PON 口检测到光信号，正在建立链路。

（c）如果处于熄灭状态，表示 PON 链路未建立连接，可能是光路不通、链路衰减过大或者设备故障。

ONU长发光故障排查

吕扬然





1. 开始

ONU 因硬件故障或软件异常,会导致不按照 OLT 分配的时隙来关闭光模块发光器,在其他 ONU 时隙还继续发光,我们称该类故障 ONU 为长发光 ONU。它将影响到 OLT 接收同一端口下的其他 ONU 的上行光信号,出现误码,甚至无法连接。虽然在实际网络中发生长发光 ONU 故障概率很低,但影响范围大。

定位故障的思路是:首先判断是否为长发光故障,然后再确认 ONU 的连接方式,最后根据长发光 ONU 特点找出故障 ONU。

2. 流程图相关操作说明

(1) 测量 OLT 端口接收光功率值是否大于−30dBm

在 OLT 侧断开光纤,使用光功率计测量 OLT 接收 1310nm 波长的光功率值。如果测量值大于−30dBm,可以确认网络中存在长发光 ONU;如果测量值小于−30dBm 或者无法读取到数值,一般为非长发光故障,有可能是大面积光纤损坏或大面积掉电等其他情况。

(2) ONU 是否通过配线架方式连接

对应如下两种方式,确认当前 ONU 是通过哪种方式连接。

① 通过分光器直连方式,如图 10-1 所示。

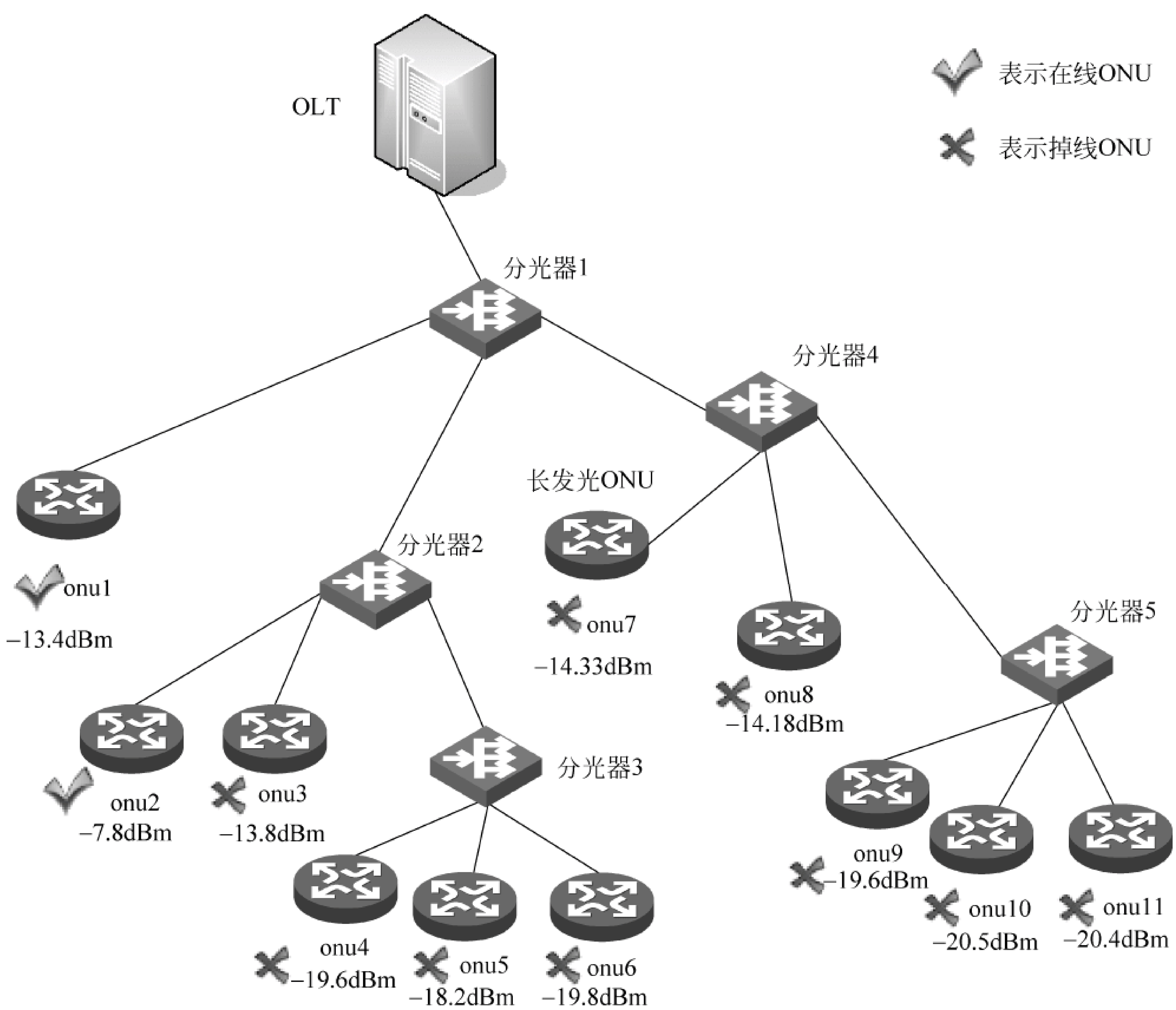


图 10-1 分光器直连方法

② 通过配线架连接方式,如图 10-2 所示。

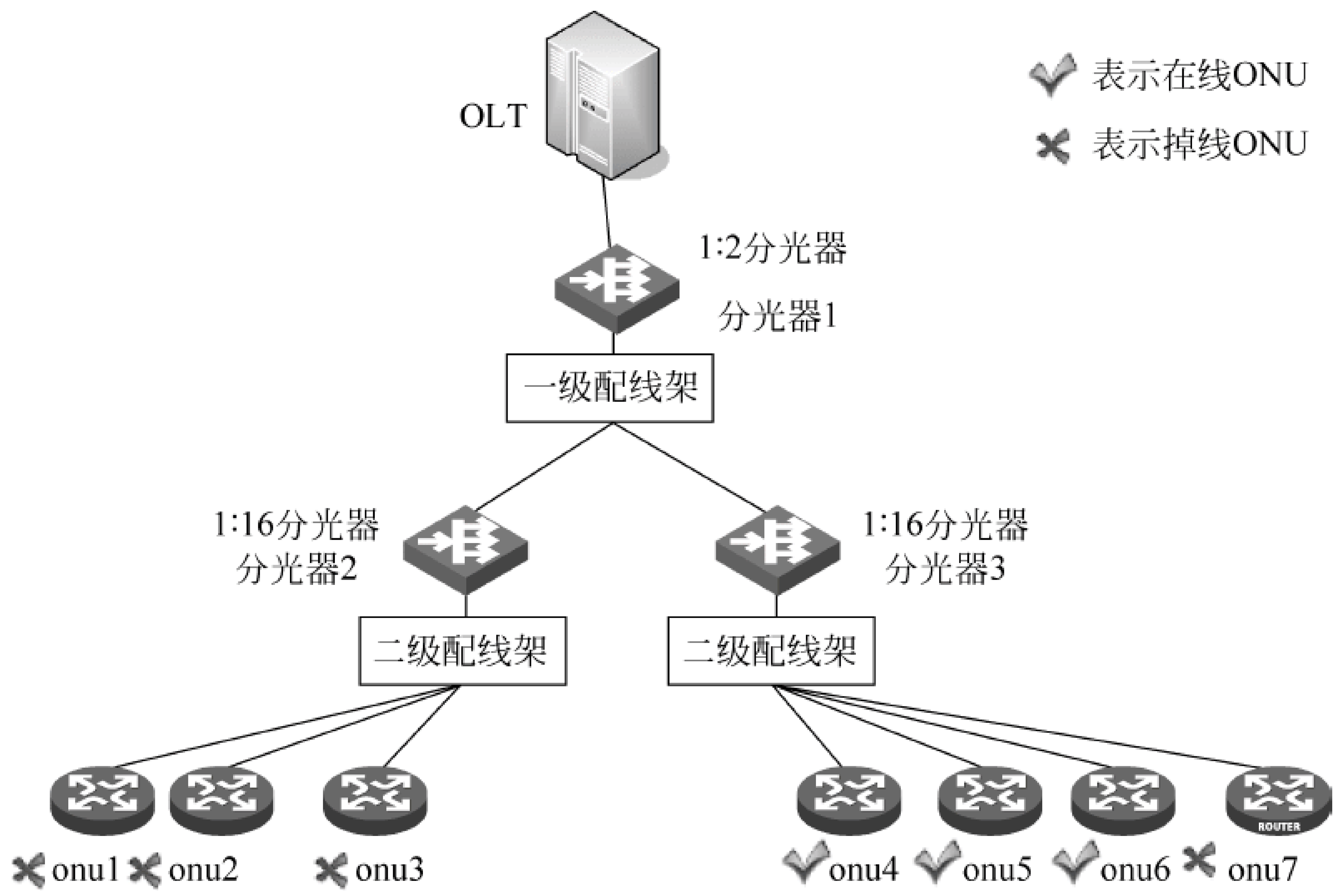


图 10-2　配线架连接方式

(3) 检查衰减最小的掉线 ONU

长发光故障 ONU 最有可能是掉线 ONU 中接收光功率值最大(即衰减最小)的那个 ONU。所以,参考实际 ONU 所在地与 OLT 之间的距离,优先排查掉线 ONU 中光衰最小、距离 OLT 最近的那台。

例如:某个 ONU 出现长发光(按 OLT 侧接收光功率值由大到小排序),如表 10-2 所示,则 2/0/1:4 和2/0/1:5 最有可能是长发光 ONU。

表 10-2　OLT 侧接收的光功率

ONU 端口号	OLT 侧接收的光功率(dBm)	状态	备　注
ONU 2/0/1:2	−7.8	在线	光功率最大的 ONU,一般为分光最大或最近的 ONU
ONU 2/0/1:1	−13.41	在线	
ONU 2/0/1:3	−13.8	在线	
ONU 2/0/1:5	−14.18	掉线	最接近在线 ONU −13.8dBm 的光功率,较大可能为长发光设备,优先排查
ONU 2/0/1:4	−14.33	掉线	最接近在线 ONU −13.8dBm 的光功率,较大可能为长发光设备,优先排查
ONU 2/0/1:6	−19.69	掉线	
ONU 2/0/1:8	−20.41	掉线	
ONU 2/0/1:7	−20.56	掉线	

(4) 插拔配线架分支线路

如图 10-3 所示,分光器 2 下掉线的 ONU 比分光器 3 下多,通过插拔一级配线架下连接分光器 2 的线路。如果拔掉后,所有掉线的 ONU 都注册上来了,则可以判断该分光器下存在长发光 ONU。

如果拔掉后,其他分光器下掉线的 ONU 依旧无法注册上来,则该分光器下没有长发光

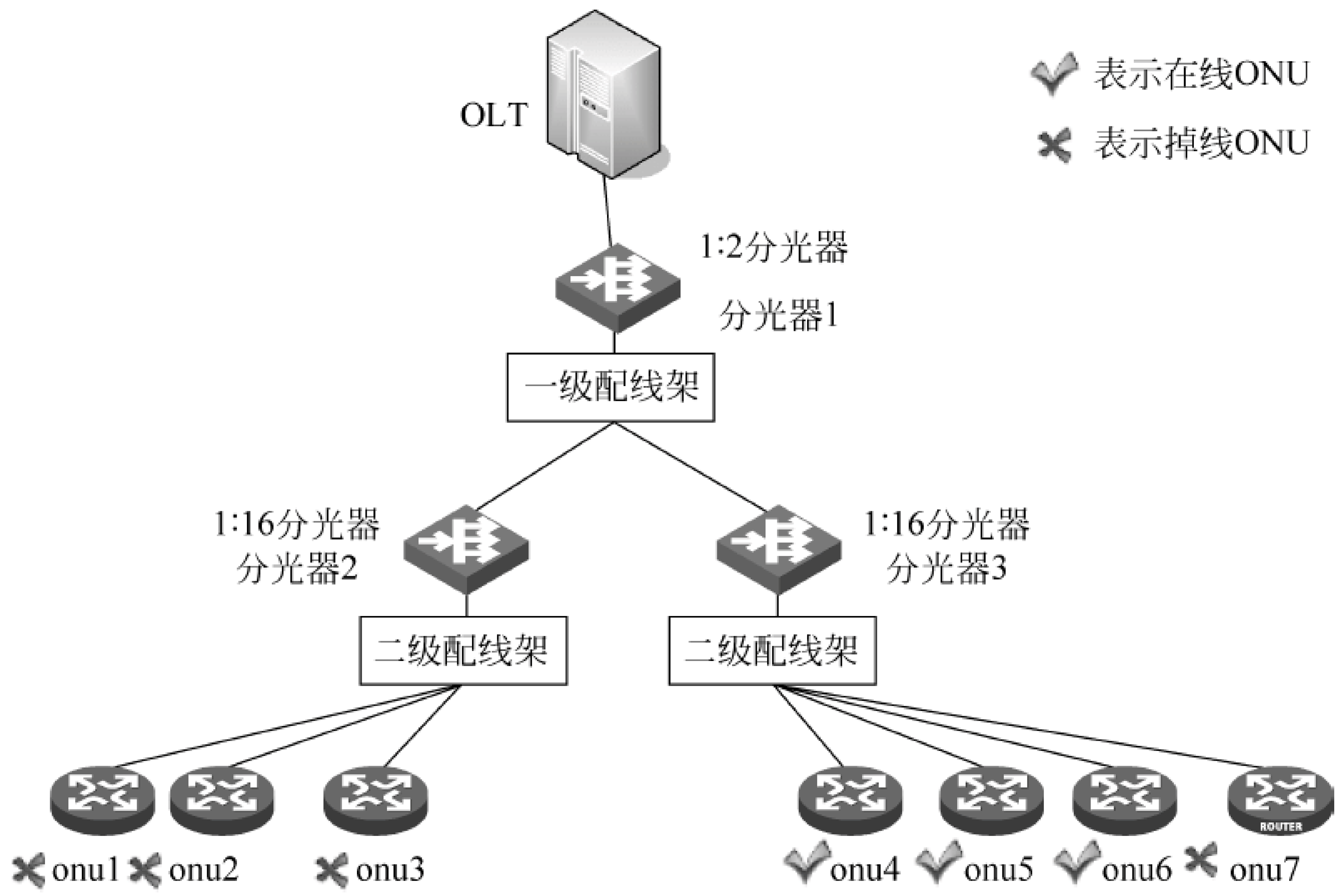


图 10-3 插拔配线架分支线路

ONU，继续插拔另外一路测试。

(5) 插拔配线架连接 ONU 的每一条光路

依次插拔配线架下连接 ONU 的每一条光路，可以判断该路下连接的 ONU 为长发光故障 ONU。如果拔掉对应的光纤，则其他掉线 ONU 能够正常注册上来。


吕扬然
OLT上无法ping通ONU的管理地址故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
查看ONU是否在线
检查ONU端口配置
检查OLT端口配置
是否在同一VLAN
检查路由可达性
使能OLT及ONU的UNI端口隔离功能
排查ONU无法注册问题
拨打热线
400-810-0504
寻求帮助

1. 开始

通过 OLT 配置 ONU 的管理地址，可以方便管理员通过 telnet 或者 Web 的方式对 ONU 进行远程管理。定位故障的思路是：先查看 ONU 是否在线，再检查 ONU 和 OLT 的相关配置是否正确，然后检查路由是否可达，最后检查是否已开启相关端口隔离功能。

2. 流程图相关操作说明

(1) 查看 ONU 是否在线

查看对应 ONU 的当前状态。

① 若当前 ONU 状态显示为 Up，说明 ONU 已经绑定，属于正常状态。

② 若当前 ONU 状态显示为 Silent，说明 ONU 处于静默状态，未在对应的 ONU 端口绑定 MAC。

③ 若当前 ONU 状态显示为 Offline，说明 ONU 已绑定 MAC，但由于绑错 MAC 地址或者其他原因导致 ONU 无法 Up。

④ 若当前 ONU 状态显示为 Down，说明 ONU 已绑定 MAC，但由于 ONU 端口被手工 Shutdown 或者其他原因导致 ONU 无法 Up。

命令：*display onuinfo slot slot-number*

例如：通过命令查看，确认当前 ONU 处于 Up 状态。

```
[H3C]display onuinfo slot 2
----------------------------------Olt2/0/1-------------------------------
ONU Mac Address   LLID  Dist(M)   Port        Board/Ver   Sft/Epm   State    Aging
000f-e2b9-cdf7     2     <1       Onu2/0/1:1  ET716/B     105/100   Up       N/A
000f-e26f-a230     1      2       Onu2/0/1:2  ET254-L/B   118/100   Up       N/A
0cda-41e3-5468     3     <1       Onu2/0/1:3  ET254-L/B   111/100   Down     N/A
0023-89b9-34a1     0     N/A      Onu2/0/1:4  N/A         N/A       Offline  N/A
000f-e2b8-2638     0     N/A         N/A      N/A         N/A       Silent   272s
```

(2) 检查 ONU 端口配置

① 查看对应 ONU 端口视图下 OLT 下发给 ONU 的配置。

命令：*display this*

例如：通过命令查看，指定 ONU 管理 VLAN 为 VLAN 10，管理地址为 192.168.10.1，网关为 192.168.10.254，ONU 端口的 PVID 为 10。

```
[H3C-Onu2/0/1:1] display this
#
interface onu2/0/1:1
bind onuid 000f-e26f-a230                 //绑定 onu 的 mac 地址
management-vlan 10                        //指定 VLAN 10 为 ONU 的管理 VLAN
undo shutdown management-vlan-interface   //打开管理 VLAN 接口
ip address 192.168.10.1 255.255.255.0 gateway 192.168.10.254   //配置管理 VLAN 接口的 IP 地址
为 192.168.10.1，网关地址为 192.168.10.254
port link-type trunk
port trunk pvid vlan 10          //ONU 端口 PVID 为 VLAN 10
#
return
```

② 若 ONU 配置的是自动获取地址，查看对应 ONU 端口视图下 OLT 下发给 ONU 的配置。

命令：*display this*

例如：通过命令查看，确认 ONU 的配置。

```
[H3C-Onu2/0/1:1] display this
#
interface onu2/0/1:1
bind onuid 000f-e26f-a230                    //绑定 onu 的 mac 地址
management-vlan 10                           //指定 VLAN 10 为 ONU 的管理 VLAN
undo shutdown management-vlan-interface      //打开管理 VLAN 接口
ip address dhcp-alloc                        //通过 DHCP 功能自动获取 IP 地址
port link-type trunk
port trunk pvid vlan 10                      //ONU 端口 PVID 为 VLAN 10
#
return
```

③ 查看对应 ONU 端口视图下当前 ONU 是否有获取到 IP 地址。

命令：*display dhcp-client*

例如：通过命令查看，ONU 作为 DHCP 客户端时获取到的管理地址为 192.168.10.3，网关为 192.168.10.254。

```
[H3C-Onu2/0/1:1]display dhcp-client
DHCP client statistic information:
Protocol status: enabled
  Current machine state : BOUND
  Allocated IP          :192.168.10.3      255.255.255.0
  Gateway IP            :192.168.10.254
  Server IP             : 192.168.10.1
```

(3) 检查 OLT 端口配置

① 查看对应 OLT 端口视图下的当前配置。

命令：*display this*

例如：通过命令查看，OLT 端口允许 VLAN 10 带 tag 通过。

```
[H3C-Olt2/0/1] display this
#
interface olt2/0/1
using onu 1 to 64
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 tagged      //允许 VLAN 10 带 tag 通过
#
return
```

② 如果 OLT 端口配置了 QinQ 功能，需要将相应的管理 VLAN 透传。

命令：*display this*

例如：通过命令查看，OLT 端口允许管理 VLAN 10 透传通过。

```
[H3C-Olt2/0/1] display this
#
interface olt2/0/1
```

```
using onu 1 to 64
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10002000 3000 tagged
qinq enable
qinq transparent-vlan10            //允许 VLAN 10 带 tag 透传通过
qos apply policy q_olt_in inbound
#
return
```

（4）是否在同一 VLAN

查看 OLT 上是否已创建与 ONU 管理 VLAN 相同的 VLAN，以及在该 VLAN 内添加相应的 VLAN 虚接口地址。

若不在同一 VLAN 内，查看路由是否可达。

（5）检查路由可达性

如果 ONU 的网关在 OLT 上，则检查 OLT 上是否已创建相应的 VLAN 虚接口，并且在 VLAN 虚接口内添加对应的地址与 ONU 的网关地址形成直连路由；若不存在，则创建相应 VLAN 虚接口。

如果 ONU 的网关在 OLT 上一级设备上，则检查 OLT 上是否有到 ONU 网关的路由；若没有，则添加相应路由，确保路由可达。

（6）使能 OLT 及 ONU 的 UNI 端口隔离功能

① 在 OLT 端口视图下使能 OLT 端口隔离功能。

命令：*port-isolate enable*

例如：通过命令使能 OLT 端口隔离功能。

```
[H3C-Olt2/0/1] port-isolate enable            //使能 OLT 端口隔离功能
```

② 在 ONU 端口视图下使能 UNI 端口隔离功能。

命令：*uni uni-number port-isolate*

例如：通过命令使能 UNI 端口隔离功能。

```
[H3C-Onu2/0/1:1] uni 1 port-isolate           //使能 UNI 1 的端口隔离功能
[H3C-Onu2/0/1:1] uni 2 port-isolate
[H3C-Onu2/0/1:1] uni 3 port-isolate
[H3C-Onu2/0/1:1] uni 4 port-isolate
```

③ 若 ONU 的型号是 ET716/ET724，需要通过如下命令使能 UNI 端口隔离功能。

命令：*onu port-isolate enable*

例如：通过命令使能 UNI 端口隔离功能。

```
[H3C-Onu2/0/1:1] onu port-isolate enable        //使能所有 UNI 的端口隔离功能
```

OLT 端口或 ONU 端口在未开启端口隔离功能的情况下，若网络中存在大量广播报文或者环路等因素，这些广播协议报文就可能会上送到 ONU 的 CPU 进行处理，导致 ONU 在短时间内 CPU 利用率提高，从而导致无法 ping 通等问题。

（7）排查 ONU 无法注册问题

参考云图《ONU 注册类问题排错》进行排查。


SMB V5交换机POE故障排查
徐 浩
表示上一步结果正常
表示上一步结果出现问题
开始
端口POE是否开启
检查端口供电功率使用
打开POE交换机非标设置
命令行开启POE功能
调整网络
收集信息反馈
拨打热线
400-810-0504
寻求帮助

1. 开始

SMB V5 交换机如下。

S2100 系列交换机、S2600 系列交换机、S3110 系列交换机、S5000PV2-EI 系列交换机、S5110 系列交换机。

POE 问题处理思路：先检查设备是否开启 POE 功能，再检查端口供电功率及整机供电功率是否超规格，再打开交换机的非标规格，最后再收集相关信息并联系 400-810-0504。

2. 流程图相关操作说明

(1) 端口 POE 是否开启

检查是否开启端口 POE 供电功能，默认设备的端口 POE 设置关闭，使用时需要命令行开启。

(2) 命令行开启 POE 功能

在对应端口视图下，开启 POE 功能。

命令：*poe enable*

(3) 检查端口供电功率使用

在命令行下查看端口及整机的 POE 使用功率，是否超规格。

命令：*display poe interface power*

(4) 调整网络

通过查看 POE 设置和 POE 使用功率，超规格需要调整网络，如调整端口最大供电功率、减少 PD 设备。

(5) 打开 POE 交换机非标设置

PD 设备分为标准 PD 和非标准 PD，标准 PD 是指符合 IEEE 802.3af 标准的 PD 设备。通常情况下，PSE 只能检测到标准 PD，并为其供电。只有在使能 PSE 检测非标准 PD 功能后，PSE 才能检测到非标准 PD，并为其供电。

命令：*poe legacy enable*

(6) 收集信息反馈

在开了非标检测后，POE 供电还是有问题的话建议收集以下信息，并联系 400-810-0504 反馈。

```
[H3C]_hid
Now you enter a hidden command view for developer's testing, some commands may
affect operation by wrong use, please carefully use it with our engineer's
direction.
[H3C-hidecmd]debug poe reg-info 1
```

查看 bank 0 配置情况。

```
[H3C-hidecmd]debug poe pse-power 1 0
```

查看 POE 端口统计信息(多查询几次方便比较结果，至少间隔 10s)。

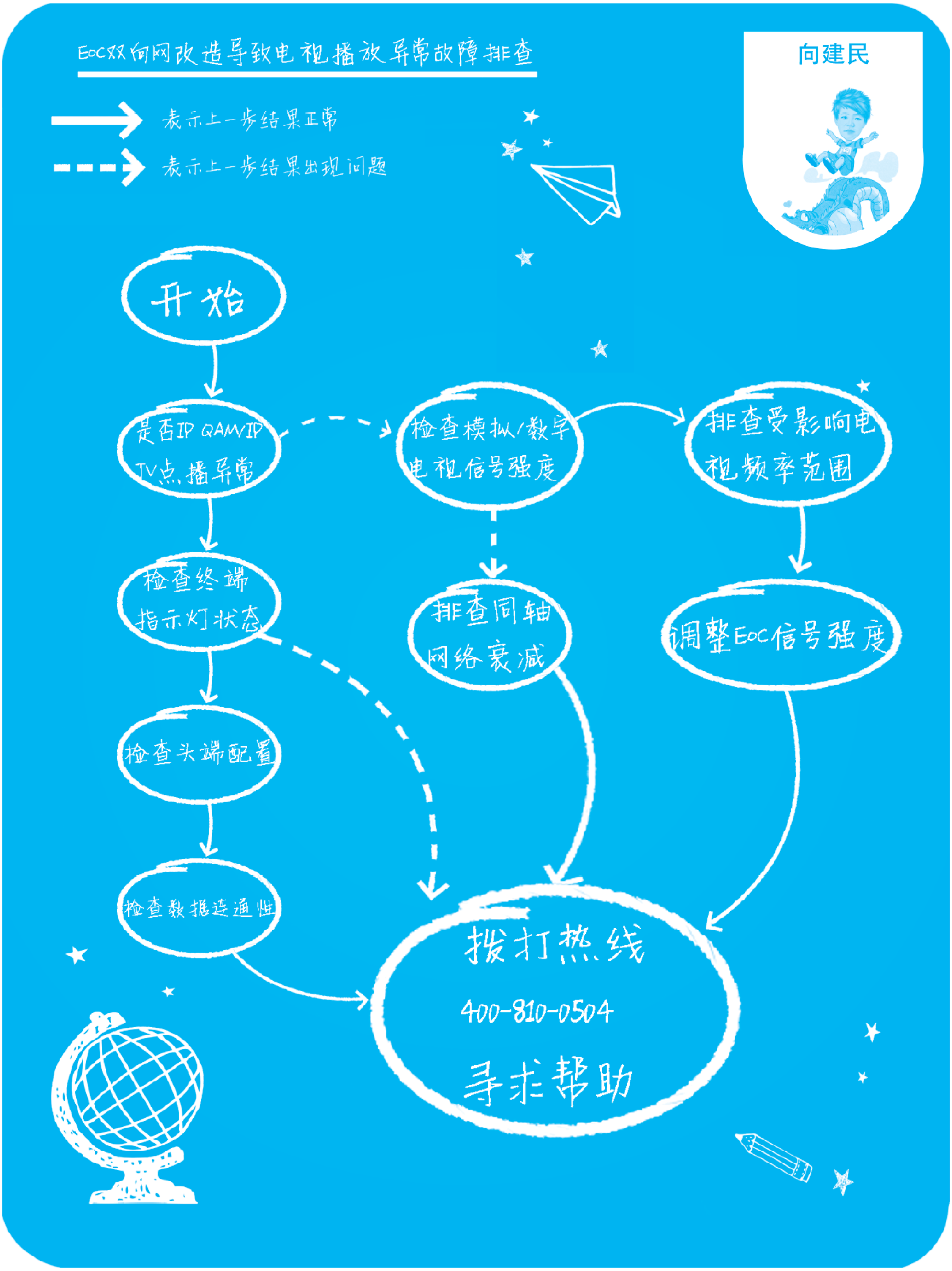
```
[H3C-hidecmd]debug poe port-mib 1
```

查看 POE 相关配置信息。

```
[H3C-hidecmd]debug poe pse-info 1
```

用命令查询扣板软件信息。

```
[H3C-hidecmd]debug poe pse-trans 2000 1
Cmd rev OK.
Respond: 20-00-02-08-01-e1-21-13-01-01-09-4b
```


EoC双向网改造导致电视播放异常故障排查
表示上一步结果正常
表示上一步结果出现问题
向建民
开始
是否IP QAM/IP TV点播异常
检查模拟/数字电视信号强度
排查受影响电视频率范围
检查终端指示灯状态
排查同轴网络衰减
调整EoC信号强度
检查头端配置
检查数据连通性
拨打热线
400-810-0504
寻求帮助

1. 开始

EPCN 是 H3C 针对广电网双向改造推出技术，是低频 EoC 技术的一种，其通过广播电视同轴网共缆传输电视信号和 EoC 数据信号。在广电进行 EoC 双向网改造时，可能会遇到改造后电视信号受影响问题。

本指导主要以排查双向网改造导致的电视播放异常，其定位故障的思路是：先判断是 IP QAM/IP TV（互动点播）异常还是模拟/数字电视（直播节目）异常，IP QAM/IP TV 异常需检查 EoC 网络的连通性，模拟/数字电视异常需依据电视信号强度和受影响的电视频率范围进行故障排查处理。

2. 流程图相关操作说明

（1）是否 IP QAM/IP TV 点播异常

检查用户反馈的电视播放异常的类型，需判断是否为 IP QAM/IP TV 的电视节目（互动点播）受影响，此类点播节目互动信号通过 EoC 进行传输，出现问题时需要进一步排查 EoC 网络。

检查点播异常现象是否为画面经常卡顿、马赛克、点播无图像等异常情况。

如果没有开通 IP QAM/IP TV 点播节目或点播无异常，则需要对模拟/数字电视业务进行排查。

（2）检查终端指示灯状态

① 检查终端 Power 灯状态。

(a) 终端的 Power 灯正常情况下处于常亮状态，如果不是说明是电源适配器输出问题或者终端故障。

(b) 检查终端电源接口是否插紧，是否正常连接。

(c) 检查插线板或者插座是否已经通电，可接上其他电器设备测试验证。

(d) 检查插线板或者插座与终端电源适配器接触是否良好。

(e) 更换一个相同型号的终端电源适配器观察是否正常。

② 检查终端 Diag 灯状态。

(a) 终端上电后，Diag 灯正常情况下处于熄灭状态。

(b) 如果亮一会后自动熄灭，说明系统正在自检、软件正在自动更新或者 Cable 链路正在自检，属于正常情况。

(c) 如果一直常亮或者闪烁，均表示终端故障，建议更换终端观察。

③ 检查终端 Cable 灯状态。

(a) 终端的 Cable 灯正常情况下处于常亮状态。

(b) 如果是一亮一灭交替闪烁，表示终端正在与头端建立连接。

(c) 如果常亮则表示终端与头端之间链路已正常建立，需要查看头端软件配置是否正确。

(d) 如果不亮则说明 Cable 链路未建立连接，可能是线路不通、链路衰减过大或终端未被授权。

（3）检查头端配置

检查头端视频业务配置是否正确，头端业务模式有 802.1Q 和透传模式两种。

透传模式下，需要重点排查终端下发模版的配置；802.1Q模式下，需重点检查视频业务VLAN设置。建议可以与业务运行正常的头端配置进行比较。

① 检查头端配置的VLAN模式。设置方法：登录头端Web管理页面，“页面向导→VLAN管理”进行设置。

VLAN模式中802.1Q和透传模式互斥；如果VLAN设置为802.1Q模式要注意是否创建有终端对应的业务VLAN ID，如图10-4所示。



图10-4　头端配置的VLAN模式

② 检查终端视频业务模板。设置方法：登录头端Web管理页面，“Cable管理”→“模板管理”→单击“新建”按钮。

业务VLAN必须成功的下发到终端的一个或几个端口，检查模板VLAN配置情况。

另外，还需要关注IP TV等视频业务端口需要关闭限速。因为EoC采取突发的方式发送数据，不建议对IP TV的端口进行限速。

例如：如图10-5所示，Cable端口不限速，Ethernet1为IP TV视频端口不限速，VLAN ID设置为1069。



图10-5　IP TV等视频业务端口限速设置

(4) 检查数据连通性

IP QAM 的点播上行回传数据流量,IP TV 的上行点播数据、下行电视节目流量,均由 EoC 网络传输,如果 EoC 网络无法通信或连接出现问题,IP QAM 表现为点播页面无反应或点播节目报错,IP TV 除以上情况外,还会出现画面卡顿和马赛克。此时需要保障 EoC 网络数据连通性正常,通常可采用以下手段判断。

① IP QAM、IP TV 的系统上查看该点播用户机顶盒是否在线正常连接。

② 在头端以太网口处接一台 FTP Server,在终端处接 PC,在出现互动点播异常问题时进行下载测试,FTP 如果未达到限速值,则可能为线路带宽不够,需要下移头端或减少头端下终端用户量。

③ 如果故障现象随机,难以复现,则可致电呼叫中心获取《EPCN 终端管理头端操作配置》,通过在终端处接 PC 长时间 ping 头端管理地址,检查 EoC 网络是否稳定。

(5) 检查模拟/数字电视信号强度

电视播放异常为模拟/数字电视直播信号,需要使用场强仪检查模拟/数字电视信号强度是否正常,判断方法如下。

① 出现故障的电视节目为模拟电视信号,需要检查模拟信号强度是否大于电视的最低接收门限,一般来说模拟电视最低接收电平 56dBuV,模拟电视信号入户标准按照大于 69dBuV±3dB 设计。

② 出现故障的电视节目为数字电视信号,需要检查数字信号强度是否大于机顶盒的最低接收门限,数字电视信号入户接收电平需大于 58dBuV±4dB。

(6) 排查同轴网络衰减

在电视接收侧使用场强仪,测试的电视信号强度小于最低接收电平,或者测量电平值远低于理论的接收电平,需要排查同轴网络的衰减问题。

① 在出现异常的电视或机顶盒处,使用场强仪测试电视信号强度,电视信号电平小于最低接收电平,并且线路上实测与理论计算的衰减相差不大,则需要调整线路,可采用如下操作。

(a) 适当减少线路上分支分配器个数,减少分支分配器衰减。

(b) 调整 Cable 同轴线缆长度,减少线路衰减。

(c) 增强电视信号源电平,调整光发射机电平。

(d) 将光发射机位置下移,缩短信号源和终端用户距离。

② 在出现异常的电视或机顶盒处,使用场强仪测试电视信号强度,电视信号电平小于最低接收电平,**并且线路上实际测试衰减远大于理论计算的衰减**,则需要从下往上,分段排查线路,可采用如下操作。

(a) 按照入户分支分配节点、楼道分支分配节点、光机节点,从下往上分段测量电平,分段排查实测衰减与理论值是否有差异。

(b) 重点排查线路上老化和松动的接头,野外的分支分配器件和用户家中的分支分配器件。

(c) 分段更换同轴线缆或新铺设线缆跳过衰减异常的线路。

(7) 排查受影响电视频率范围

确认受影响的电视频段范围,可通过场强仪或频谱分析仪接驳高通滤波器在受影响节点进行测试。根据直播电视频段划分,可将受影响电视范围分为以下几种类型。

① 低频段(50～80MHz 频段范围)模拟电视信号受到干扰,其他频段电视节目不受干扰。

其原因未按照国标 GY/T 106—1999《有线电视广播系统技术规范》标准使用电视频段，需将低频段电视节目移至 110MHz 以上。

② 特定频段电视信号干扰，其受干扰的节目在某个特定频段，一般为有源设备引入，可能是机顶盒、线路异常串扰进入的电磁干扰(电瓶车充电器)、异常的 EoC 设备等。排查方法可以在出现干扰的频点使用频谱分析仪，并将线路上和线路周边有源设备依次下电查找干扰源。

③ 全频段干扰，直播电视节目全部频道受到干扰，表现为全部数字电视出现马赛克，模拟电视出现雪花干扰，场强仪测试节目误码率高。此情况一般为线路信号质量较好，EoC 信号较强，而终端机顶盒或电视没有内置高通滤波器或滤波器件过滤信号不够造成，需要增加 EoC 信号衰减或过滤 EoC 信号。

(8) 调整 EoC 信号强度

受影响电视为全频段干扰，下电 EoC 头端设备后即可恢复，一般情况为 EoC 信号质量较强，而终端机顶盒或电视没有内置高通滤波器或滤波器件过滤信号不够造成，一般可以采取以下方式调整解决。

① 在出现问题的机顶盒或电视处增加高通滤波器，过滤 EoC 信号，如图 10-6 所示。

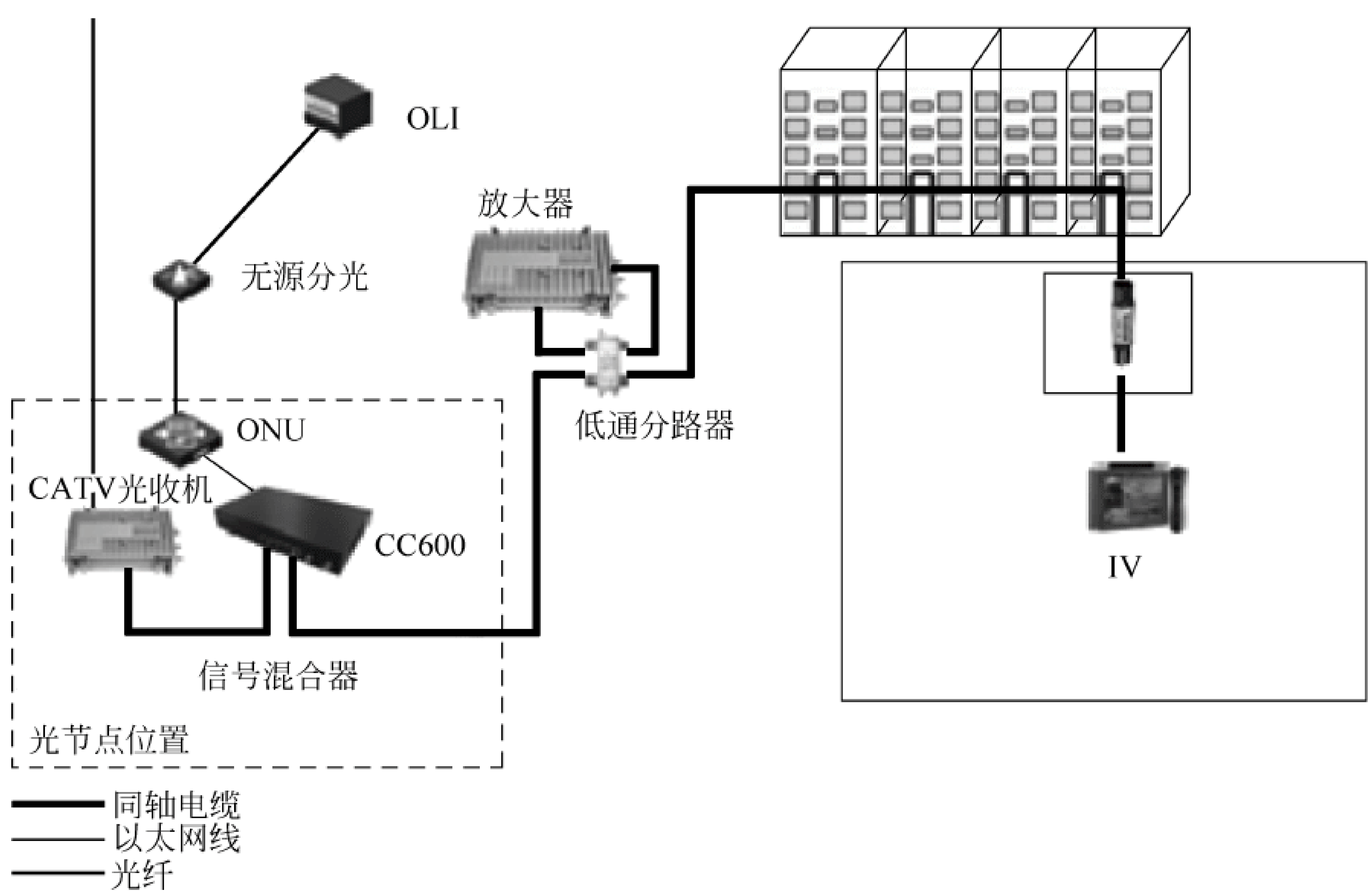


图 10-6 调整 EoC 信号强度

② 调整 EoC 头端输出功率，建议调整范围为 5～10dB。登录 Web 页面，“页面向导：Cable 管理→功率调整”，如图 10-7 所示。如果该头端 Web 页面没有“功率调整”菜单，请联系呼叫中心处理。

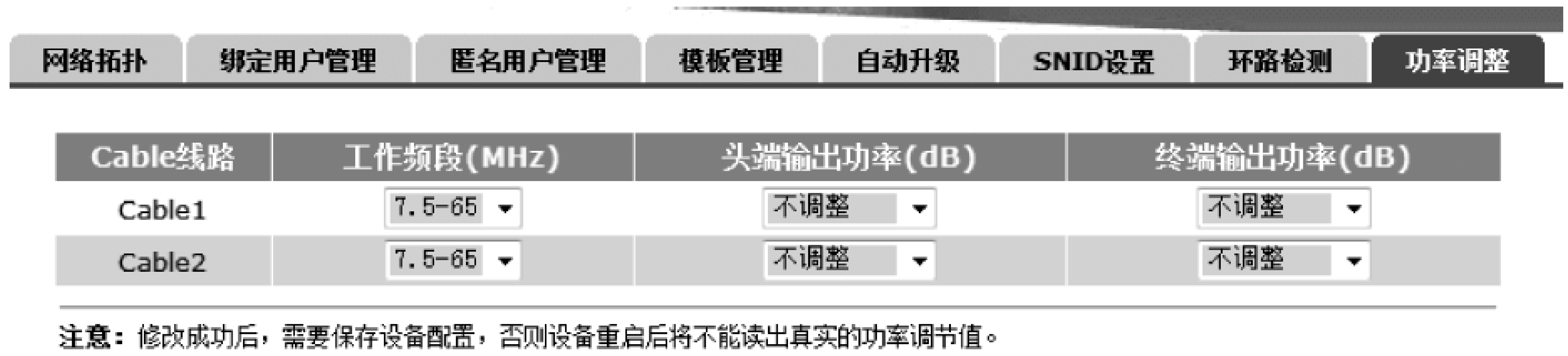
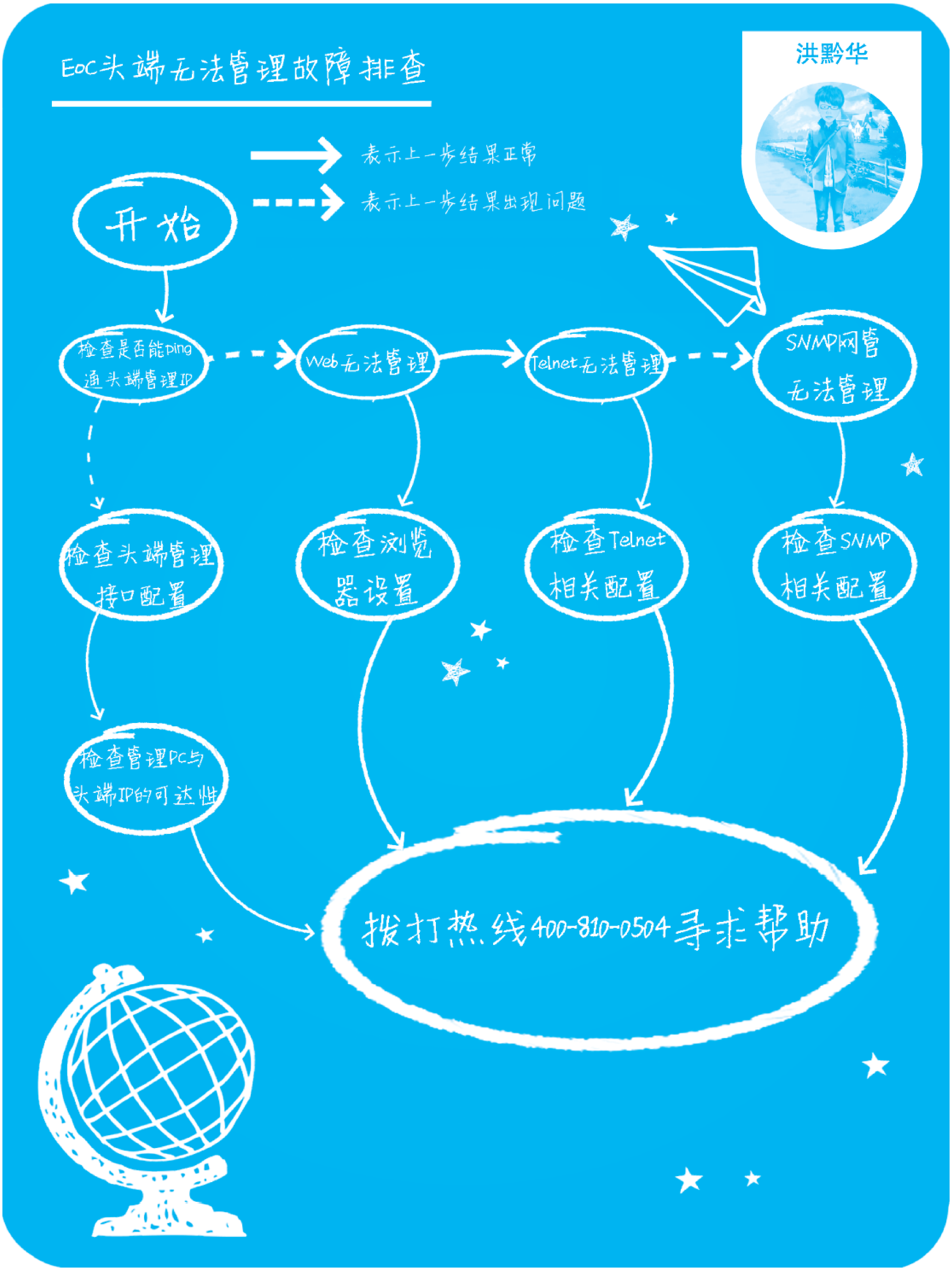


图 10-7 EoC 头端输出功率调整


EoC头端无法管理故障排查
洪黔华
表示上一步结果正常
表示上一步结果出现问题
开始
检查是否能ping通头端管理IP
Web无法管理
Telnet无法管理
SNMP网管无法管理
检查头端管理接口配置
检查浏览器设置
检查Telnet相关配置
检查SNMP相关配置
检查管理PC与头端IP的可达性
拨打热线400-810-0504寻求帮助

1. 开始

EPCN 是 H3C 针对广电接入网双向改造推出的技术，是低频 EoC 技术的一种，通过广播电视同轴网共缆传输电视信号和 EoC 数据信号。EoC 头端的管理方式包括 Console 口、Web、Telnet、SNMP 等，Console 口无法管理问题，大多与硬件故障有关，可替换设备观察；其他管理方式问题，定位故障的思路是：首先确认管理 PC 与头端之间的连通性，然后再根据管理类型检查相关配置。

2. 流程图相关操作说明

(1) 检查是否能 ping 通头端管理 IP

打开管理 PC 的命令提示符窗口，ping 头端的管理 IP 地址(默认地址为 192.168.0.241)，确认是否能正常 ping 通。

例如：管理 PC ping 头端管理地址 192.168.0.241 正常无丢包。

```
C:\>ping 192.168.0.241

正在 ping 192.168.0.241 具有 32 字节的数据:
来自 192.168.0.241 的回复:字节=32 时间=16ms TTL=64
来自 192.168.0.241 的回复:字节=32 时间<1ms TTL=64
来自 192.168.0.241 的回复:字节=32 时间<1ms TTL=64
来自 192.168.0.241 的回复:字节=32 时间<1ms TTL=64

192.168.0  .241 的 ping 统计信息:
    数据包:已发送= 4,已接收= 4,丢失= 0 (0%丢失),
往返行程的估计时间(以毫秒为单位):
    最短= 0ms,最长= 16ms,平均= 4ms
```

(2) 检查头端管理接口配置

① 检查头端管理 VLAN 是否配置正确。

通过 Console 口登录头端设备，查看头端管理 VLAN 是否与规划一致。

命令：*display current-configuration*

例如：通过命令查看，可以确认头端的管理 VLAN 为 99。

```
<H3C>display current-configuration
#
 version104
#
 sysname H3C
#
 management-vlan 99
#
…
```

② 检查头端 IP 地址是否配置正确。

通过 Console 口登录头端设备，查看头端管理 VLAN 接口下的 IP 地址、子网掩码、网关地址配置是否正确。

命令：*display interface vlan-interface vlanid*

例如：通过命令查看，可以确认头端 99 管理 VLAN 接口 IP 地址为 192.168.0.241，子网掩码为 255.255.255.0，网关地址为 192.168.0.1(默认情况下网关没有指定)。

```
<H3C>display interface vlan-interface 99
Vlan-interface99 current state: Up
Line protocol current state: Up
Hardware address is 5866-baf4-3878
Internet address is 192.168.0.241/24
Gateway address is 192.168.0.1
The Maximum Transmit Unit is 1500
Description : Vlan-Interface99 Interface
```

③ 远程管理情况下，检查头端级联端口 VLAN 配置。

如果头端上行采用以太网口级联，通过 Console 口登录头端设备，查看头端级联以太网端口的 VLAN 配置是否已经允许管理 VLAN 通过了。

命令：*display current-configuration*

例如：通过命令查看，可以确认头端的以太网端口处于 VLAN 透传模式下的 Transparent 模式，管理 VLAN 报文可以带标签正常转发。

```
<H3C>display current-configuration
...
#
interface GigabitEthernet1/1/1
 port vlantransmode untag
 port access vlan 99
#
interface GigabitEthernet1/1/2
 port vlantransmode transparent
#
...
```

或者可以确认头端工作在 802.1Q 模式下的以太网端口已经允许管理 VLAN 带标签通过了。

```
<H3C>display current-configuration
...
#
interface GigabitEthernet1/1/1
 port access vlan 99
#
interface GigabitEthernet1/1/2
 port link-type trunk
 port trunk permit vlan 1 99 1001 2011
#
...
```

如果头端上行采用 PON 口级联，还需要登录 OLT 设备，查看头端 ONU 端口的 VLAN 配置是否已经配置为 Trunk 模式了。

例如：通过命令查看，可以确认头端 ONU 端口已经配置为 Trunk 模式了，管理 VLAN 报文可以带标签正常转发。

```
[H3C-Onu2/0/1:1]display this
#
 interface onu2/0/1:1
 descriptionLantianxiaoqu 3#2-Danyuan
 bind onuid 000f-e26f-a230
 upstream-sla maximum-bandwidth 16000
 port link-type trunk
#
```

④ 本地管理情况下，检查头端本地连接 PC 的以太网端口配置。

如果头端上行采用以太网口级联，通过 Console 口登录头端设备，查看头端以太网端口的 VLAN 配置是否正确。

命令：*display current-configuration*

例如：通过命令查看，可以确认头端的以太网端口处于 VLAN 透传模式下的 Untag 模式。

```
<H3C>display current-configuration
...
#
interface GigabitEthernet1/1/1
 port vlantransmode untag
 port access vlan 99
#
interface GigabitEthernet1/1/2
 port vlantransmode transparent
```

或者可以确认头端工作在 802.1Q 模式下的以太网端口已经允许管理 VLAN 不带标签通过了。

```
<H3C>display current-configuration
...
#
interface GigabitEthernet1/1/1
 port access vlan 99
#
interface GigabitEthernet1/1/2
 port link-type trunk
 port trunk permit vlan 1 99 1001 2011...
```

(3) 检查管理 PC 与头端 IP 地址可达性

① 检查管理 PC 的 IP 地址、子网掩码、网关配置情况。

通过管理 PC 的命令提示符窗口查看本地网卡的 IP 地址、子网掩码配置与头端管理 IP 是否属于相同网段。

例如：打开管理 PC 的命令提示符窗口，输入“ipconfig /all”显示以太网适配器本地连接中的 IP 地址为 192.168.0.12，掩码为 255.255.255.0。

```
C:\>ipconfig /all
以太网适配器  本地连接:
   连接特定的 DNS 后缀. . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connecti
on
   物理地址. . . . . . . . . . . . . : A0-B3-CC-23-AA-D0
   DHCP 已启用. . . . . . . . . . . :否
```

```
自动配置已启用. . . . . . . . . . . : 是
IPv4 地址. . . . . . . . . . . . . . : 192.168.0.12(首选)
子网掩码  . . . . . . . . . . . . . : 255.255.255.0
默认网关. . . . . . . . . . . . . . :
TCPIP 上的 NetBIOS  . . . . . . : 已启用
```

如果管理 PC 跨网段访问头端，则还需要检查管理 PC 和头端的网关地址配置正确性。

例如：打开管理 PC 的命令提示符窗口，输入“ipconfig /all”显示以太网适配器本地连接中的 IP 地址为 192.168.9.12，网关地址为 192.168.9.1。

```
C:\>ipconfig /all
以太网适配器  本地连接:
  连接特定的 DNS 后缀. . . . . . . :
  描述. . . . . . . . . . . . . . .  : Intel(R) 82579LM Gigabit Network Connecti
on
  物理地址. . . . . . . . . . . . .  : A0-B3-CC-23-AA-D0
  DHCP 已启用. . . . . . . . . . . : 否
  自动配置已启用. . . . . . . . . . : 是
  IPv4 地址. . . . . . . . . . . .  : 192.168.9.12(首选)
  子网掩码  . . . . . . . . . . . . : 255.255.255.0
  默认网关. . . . . . . . . . . . . .:.192.168.9.1
  TCPIP 上的 NetBIOS  . . . . . . : 已启用
```

② 检查头端本地或上连端口的工作状态。

通过 Console 口登录头端设备，查看头端本地或上连端口是否 Up，协商是否正确，对于采用 PON 口上连的头端，可以登录 OLT 查看 ONU 口的状态。

命令：*display interface*

例如：通过命令查看，可以确认头端本地或上连以太网端口处于 Up，且工作在 1000M/FULL 状态。

```
<H3C>display interface GigabitEthernet 1/1/1
GigabitEthernet1/1/1 current state: Up
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0023-89cc-712e
Media type is twisted pair
Port hardware type is 1000_BASE_T
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
…
```

如果头端采用 PON 口上连，需确认 ONU 口处于 Up 状态。

```
<H3C>display interface Onu2/0/1:1
Onu2/0/1:1 current state: Up
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: c4ca-d9e0-0e68
 Description: Onu2/0/1:1 Interface
 The Maximum Frame Length is 1600
…
```

③ 检查 PC 与头端的 ARP 学习情况。

打开管理 PC 的命令提示符窗口，使用“arp -a”命令查看管理 PC 的 ARP 学习情况。

例如：如果管理 PC 与头端 IP 在相同网段，在管理 PC 上查看 ARP，已经正确学习到了头

端的管理 IP 对应的 ARP。

```
C:\>arp -a
...
接口: 192.168.0.12 --- 0x1d
  Internet      地址           物理地址               类型
  192.168.0    .241         00-23-89-cc-71-2e       动态
```

再查看头端的 ARP 表项，在管理 VLAN 中学习到了管理 PC 的 ARP。

```
<H3C>display arp
IP Address           MAC Address          VLAN ID   Aging
192.168.0.12         a0b3-cc23-aad0       99        16
--- 1 entry(ies) found ---
```

如果管理 PC 与头端 IP 不在相同网段，在管理 PC 上查看 ARP，已经学习到了网关地址对应的 ARP。

```
C:\>arp -a
...
接口: 192.168.9.12 --- 0x1d
  Internet 地址        物理地址              类型
  192.168.9.1         c4-ca-d9-e0-17-e2      动态
```

再查看头端的 ARP 表项，在管理 VLAN 中学习到了网关地址对应的 ARP。

```
<H3C>display arp
IP Address          MAC Address         VLAN ID   Aging
192.168.0.1         c4ca-d9e0-0e68      99        16
--- 1 entry(ies) found ---
```

(4) Web 无法管理

打开浏览器，在地址栏里输入头端的管理地址，打开设备管理页面，确认是否为无法打开设备管理或打开后无法登录 Web 界面操作。

(5) 检查浏览器设置

① 检查 IE 浏览器是否设置了代理。

在浏览器窗口中，单击“工具”按钮→单击“Internet 选项”命令，在弹出的窗口中选择“连接”选项卡，并单击“局域网(LAN)设置”按钮，进入如图 10-8 所示页面，确认取消选中“为 LAN 使用代理服务器”复选框；若已选中，请取消选中并单击“确定”按钮。

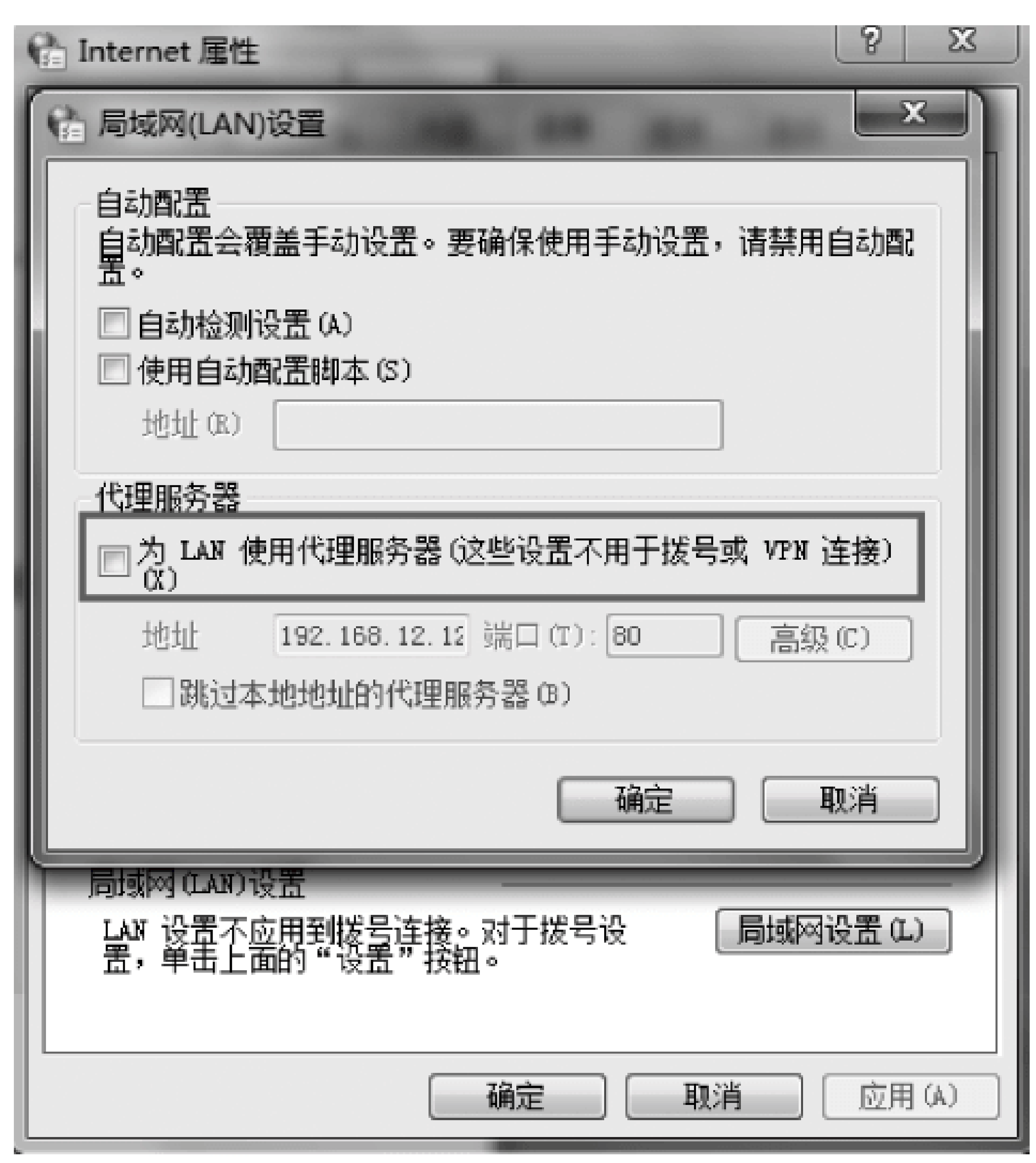


图 10-8 浏览器设置

② 更换浏览器或者使用另一台管理 PC 上的浏览器访问头端的 Web 管理页面。

③ 登录管理页面输入密码时，请确认大写是否锁定；如忘记密码，可单击登录页面的“忘记密码”按钮按照提示恢复，如图 10-9 所示。

(6) Telnet 无法管理

在 PC 系统中的“开始”→“运行”中输入



图 10-9 管理页面

CMD 命令，打开命令提示符，或通过专用的终端软件（例如 CRT 等），Telnet 头端的管理地址，确认是否能正常登录头端。

（7）检查 Telnet 相关配置

通过 Console 口登录头端设备，查看头端 Telnet 相关配置。

命令：*display current-configuration*

例如：通过命令查看，可以确认头端 Telnet Server 已开启（默认配置不显示，Telnet Server 关闭才会显示），用户接口 VTY0 下配置了认证模式和认证密码。

```
[H3C]telnet server enable
Info: Telnet server has been started!
[H3C] display current-configuration
…
user-interface vty 0
 set authentication password simple admin
user-interface vty 1
```

（8）SNMP 网管无法管理

通过 SNMP 网管软件（例如 IMC 等）按照配置的 SNMP 参数连接头端的管理地址，确认是否可以正常连接。

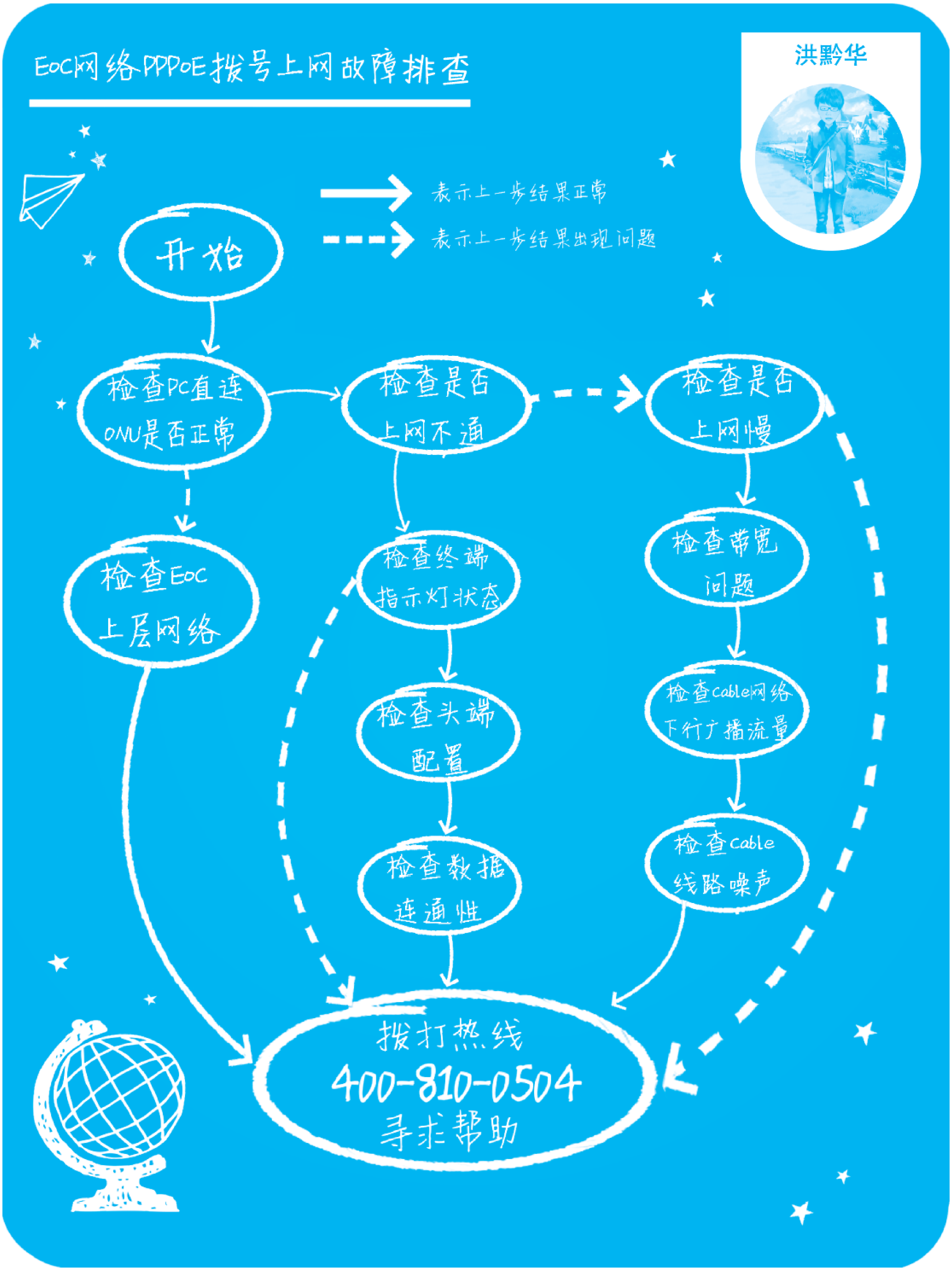
（9）检查 SNMP 相关配置

通过 Console 口登录头端设备，查看头端 Telnet 相关配置。

命令：*display current-configuration*

例如：通过命令查看，可以确认头端 SNMP 已经开启，读写团体名为 Public/Private，SNMP 版本号为 V2C，Trap 已经开启并指定了 192.168.100.10 为发送主机地址。

```
[H3C] display current-configuration
…
#
 snmp-agent
 snmp-agent local-engineid 800063A24567002389CC712E
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info version v2c
 snmp-agent trap enable
 snmp-agent target-host trap address udp-domain 192.168.100.10 permit params securityname public
v2c event all permit
#
```


EoC网络PPPoE拨号上网故障排查
洪黔华
表示上一步结果正常
表示上一步结果出现问题
开始
检查PC直连ONU是否正常
检查是否上网不通
检查是否上网慢
检查EoC上层网络
检查终端指示灯状态
检查头端配置
检查数据连通性
检查带宽问题
检查cable网络下行广播流量
检查cable线路噪声
拨打热线
400-810-0504
寻求帮助

1. 开始

EPCN 是 H3C 针对广电接入网双向改造推出的技术，是低频 EoC 技术的一种，通过广播电视同轴网共缆传输电视信号和 EoC 数据信号。基于广电 EoC 技术的网络，上网通常采用 PPPoE 拨号方式，上网异常问题一般可分为上网不通和上网慢两类，定位故障的思路是：首先将测试 PC 直连 EoC 头端设备上连的 ONU，在 ONU 的以太网口上配置正确的上网业务 VLAN 信息，观察此时测试 PC 拨号上网是否正常，确认 EoC 上层网络不存在问题，然后再根据 EoC 网络引起的上网异常类型来排查；上网不通故障可先检查头端配置，再检查链路连通性；上网慢故障可先检查 Cable 网络下行是否存在大流量广播报文，然后检查 Cable 线路噪声问题。

2. 流程图相关操作说明

(1) 检查 PC 直连 ONU 是否正常

测试 PC 直连 EoC 头端上连 ONU 空闲的以太网口，将该端口配置为 Tag 模式的上网业务 VLAN，观察此时测试 PC 采用客户账号或测试账号拨号上网是否正常。

① 如果此时测试 PC 上网依旧存在问题，建议排查 EoC 上层网络问题。

② 如果此时测试 PC 上网一直正常，而客户处上网依旧存在问题，需要进一步排查 EoC 网络。

(2) 检查 EoC 上层网络

EoC 上层网络建议排查以下内容。

① 检查上层网络(如 EPON 网络等)的配置是否正确。

② 检查端口隔离是否已经开启。

③ 检查广播域是否过大。

④ 检查上层链路延迟是否正常。

⑤ 检查拨号服务器是否正常。

⑥ 检查带宽是否足够等。

(3) 检查是否上网不通

确认客户 PC 拨号是否连接不上。

(4) 检查终端指示灯状态

① 检查终端 Power 灯状态。

(a) 终端的 Power 灯正常情况下处于常亮状态，如果不是说明电源适配器输出问题或者终端故障。

(b) 检查终端电源接口是否插紧，是否正常连接。

(c) 检查插线板或者插座是否已经通电，可接上其他电器设备测试验证。

(d) 检查插线板或者插座与终端电源适配器接触是否良好。

(e) 更换一个相同型号的终端电源适配器观察是否正常。

② 检查终端 Diag 灯状态。

(a) 终端上电后，Diag 灯正常情况下处于熄灭状态。

(b) 如果亮一会后自动熄灭，说明系统正在自检、软件正在自动更新或者 Cable 链路正在

自检，属于正常情况。

(c) 如果一直常亮或者闪烁，均表示终端故障，建议更换终端观察。

③ 检查终端 Cable 灯状态。

(a) 终端的 Cable 灯正常情况下处于常亮状态。

(b) 如果是一亮一灭交替闪烁，表示终端正在与头端建立连接。

(c) 如果常亮则表示终端与头端之间链路已正常建立，需要查看头端软件配置是否正确。

(d) 如果不亮则说明 Cable 链路未建立连接，可能是线路不通、链路衰减过大或终端未被授权。

(5) 检查头端配置

① 检查头端 VLAN 配置。

进入头端设备 Web 管理界面→"VLAN 管理"→"VLAN 透传"，检查当前 VLAN 透传功能处于开启还是关闭状态；如果 VLAN 透传功能开启，检查头端用于级联的上行以太网端口出口报文类型是否为透传模式，如图 10-10 所示。

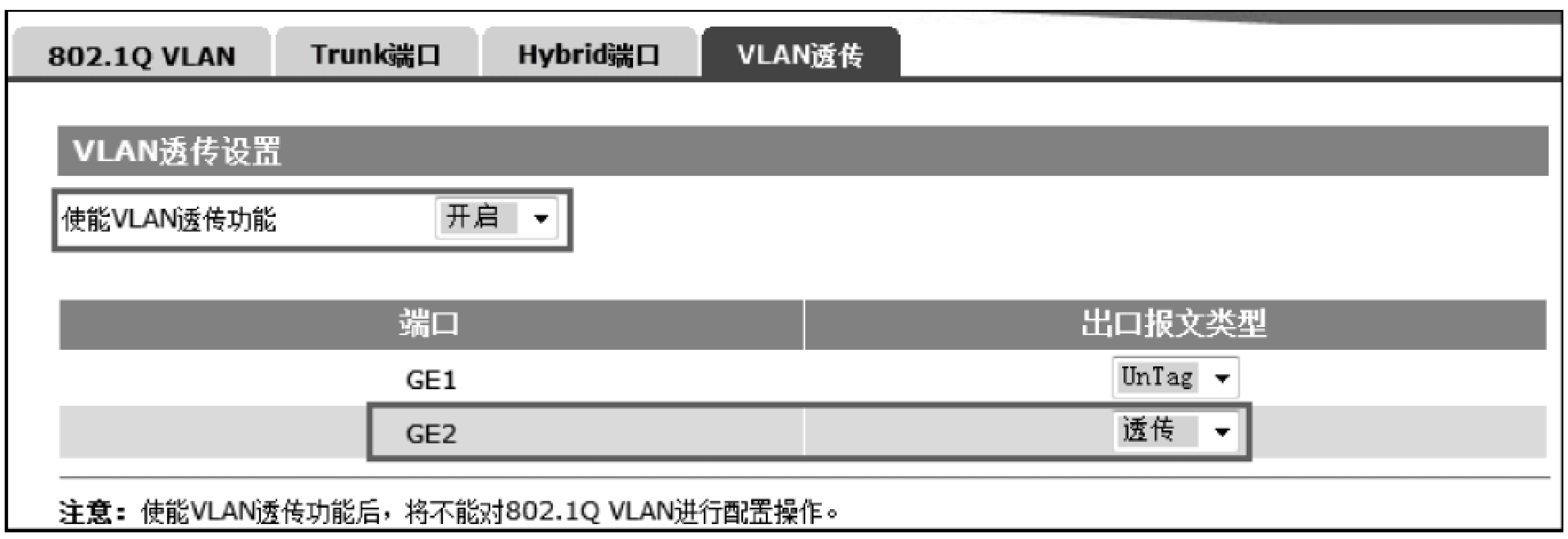


图 10-10 头端配置检查

如果 VLAN 透传功能关闭，如图 10-11 所示，说明当前 VLAN 模式处于 802.1Q VLAN 模式，检查头端是否已经创建了上网业务的 VLAN ID，如图 10-12 所示，头端用于级联的上行以太网端口是否已经配置为 Trunk 端口并允许上网业务 VLAN 通过了，如图 10-13 所示。

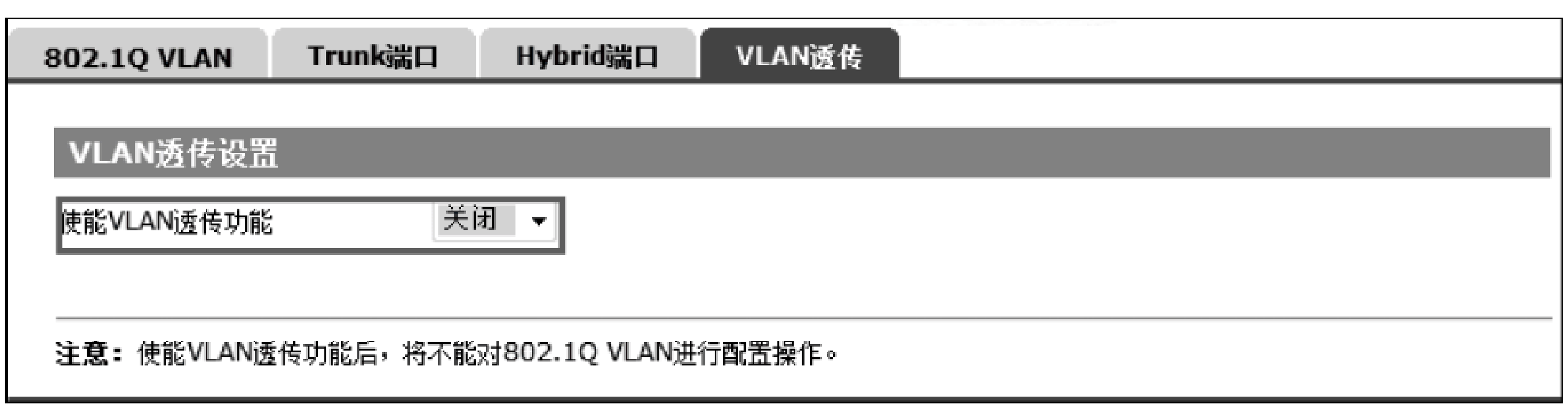


图 10-11 VLAN 透传功能关闭

② 检查终端 VLAN 配置。

进入头端设备 Web 管理界面→"Cable 管理"→"网络拓扑"，单击该上网不通用户终端的"用户名"超链接进入终端用户管理页面，"模板选择"配置项中选择"无模板"下拉列表框，检查终端接 PC 的以太网 2 口的速率、双工模式是否为自协商，端口是否开启，是否正确配置了上网业务的 VLAN，如图 10-14 所示。

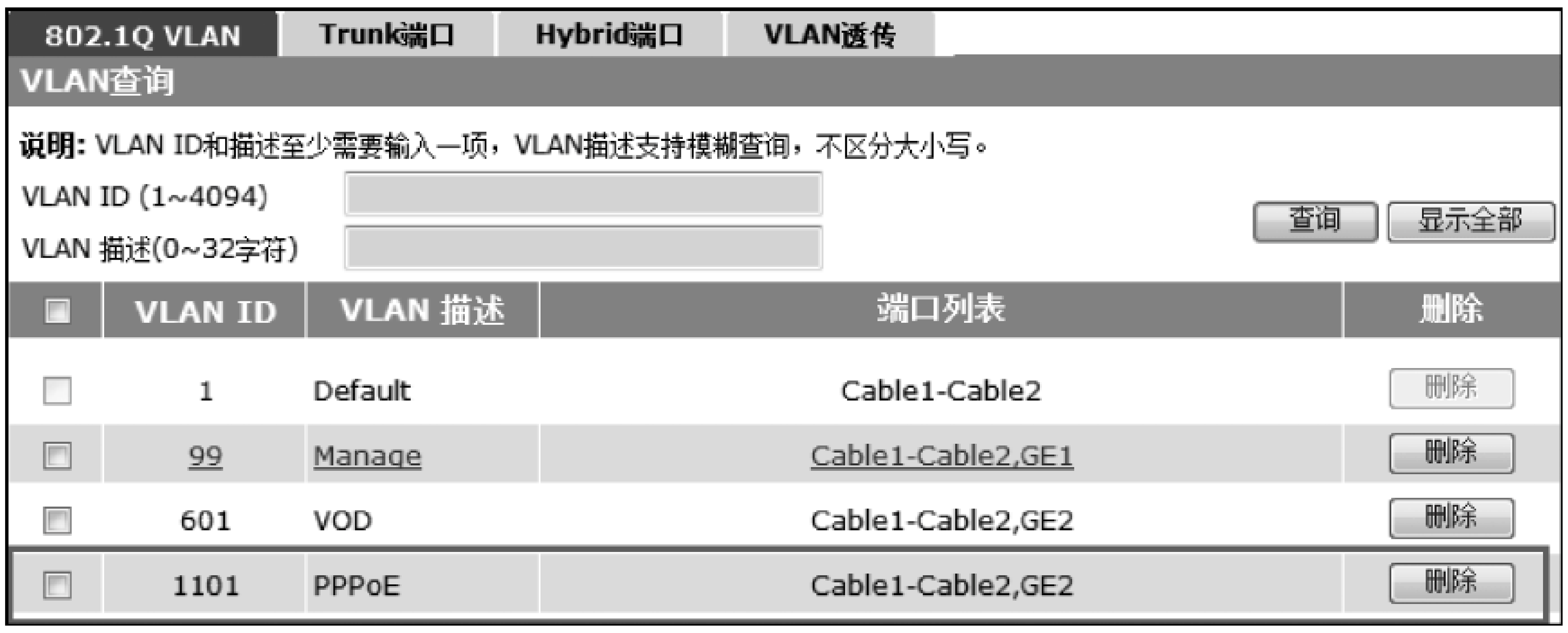


图 10-12　上网业务的 VLAN ID

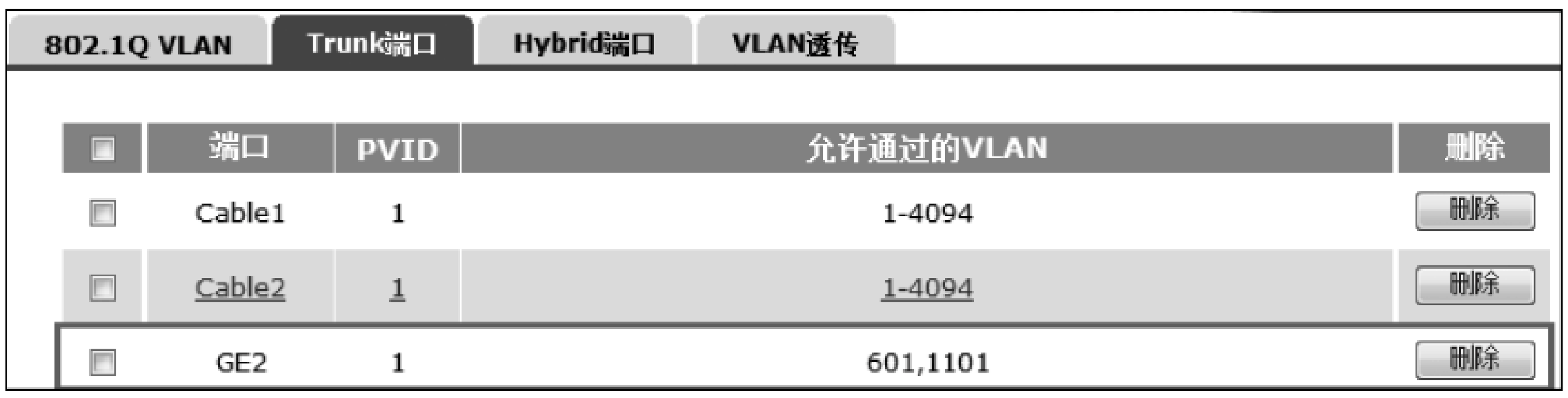


图 10-13　Trunk 端口配置



图 10-14　终端 VLAN 配置

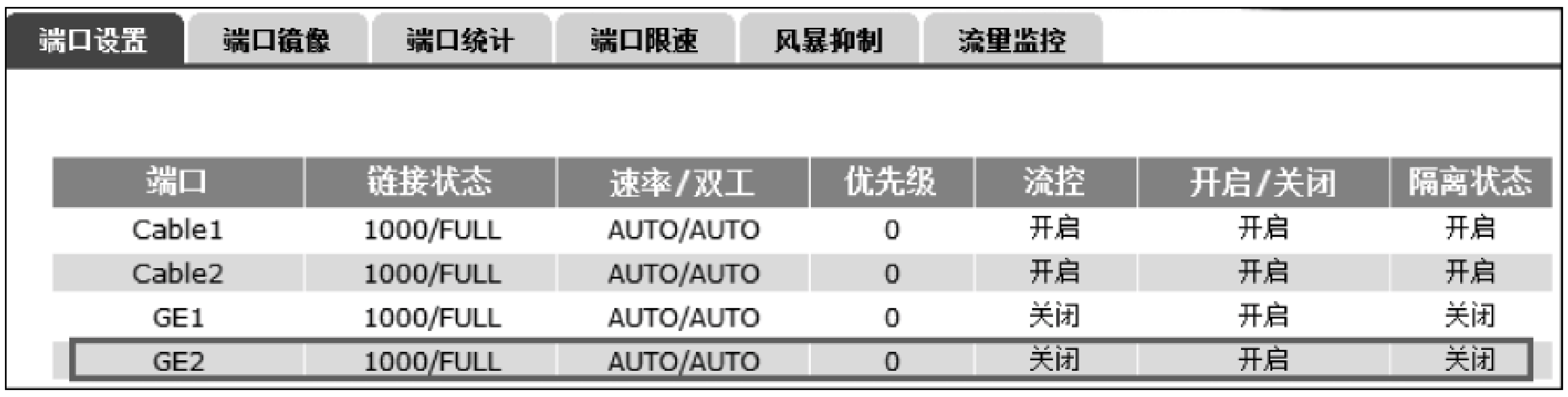
(6) 检查数据连通性

① 检查客户 PC 是否能 ping 通网关地址。

将客户 PC 网卡配置为上网业务 VLAN 网段的静态 IP 地址，打开 PC 的命令提示符窗口，ping 网关地址，确认是否能正常 ping 通。

② 检查头端级联口状态。

如果头端上行是以太网口级联，进入头端设备 Web 管理界面→“端口管理”→“端口设置”，查看头端上行以太网口“速率/双工”是否处于 AUTO/AUTO 状态，链路状态是否正常，如图 10-15 所示。



端口	链接状态	速率/双工	优先级	流控	开启/关闭	隔离状态
Cable1	1000/FULL	AUTO/AUTO	0	开启	开启	开启
Cable2	1000/FULL	AUTO/AUTO	0	开启	开启	开启
GE1	1000/FULL	AUTO/AUTO	0	关闭	开启	关闭
GE2	1000/FULL	AUTO/AUTO	0	关闭	开启	关闭

图 10-15 头端上行以太网口“速率/双工”状态

如果头端上行是 PON 口级联，进入头端设备 Web 管理界面→“系统管理”→“PON 信息”(如果是 CC754，需要进入 ONU 管理页面查看)，查看头端上行 PON 口的连接状态是否为“已连接”或者“在线”状态，光接收功率是否处于－24dBm 到－8dBm 之间，如图 10-16 所示。

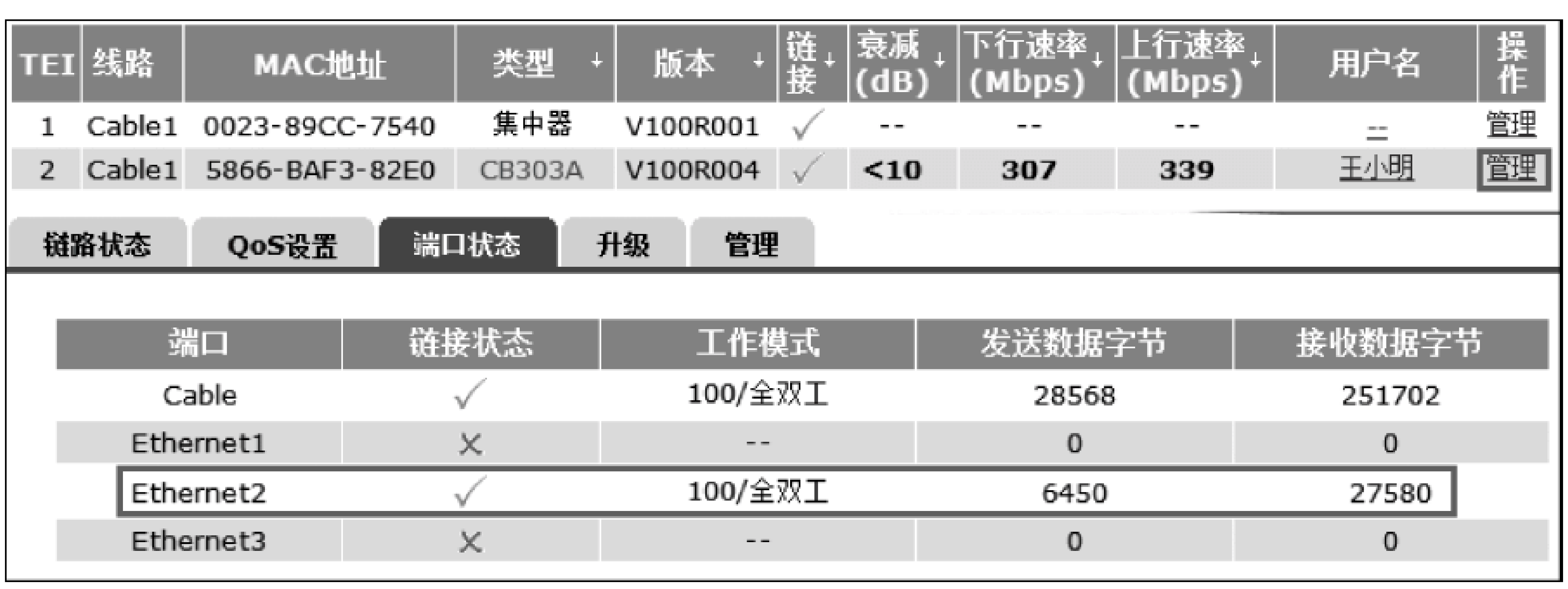


PON状态	已连接
OAM状态	已连接
光模块状态	开启
逻辑链路ID	3
接收光功率	-18.92dBm
发送光功率	1.75dBm

图 10-16 PON 状态

③ 检查终端连接 PC 端口的连接状态。

进入头端设备 Web 管理界面→“Cable 管理”→“网络拓扑”，单击该上网不通用户终端的“管理”超链接进入终端设备管理页面，选择“端口状态”页面查看终端连接 PC 的以太网口链接状态和工作模式是否正常，如图 10-17 所示。



TEI	线路	MAC地址	类型	版本	链接	衰减(dB)	下行速率(Mbps)	上行速率(Mbps)	用户名	操作
1	Cable1	0023-89CC-7540	集中器	V100R001	✓	--	--	--	--	管理
2	Cable1	5866-BAF3-82E0	CB303A	V100R004	✓	<10	307	339	王小明	管理

端口	链接状态	工作模式	发送数据字节	接收数据字节
Cable	✓	100/全双工	28568	251702
Ethernet1	×	--	0	0
Ethernet2	✓	100/全双工	6450	27580
Ethernet3	×	--	0	0

图 10-17 终端连接 PC 端口的连接状态

④ 检查客户 PC 网卡状态是否正常，PPPoE 拨号软件是否正常。

将客户 PC 网卡尝试禁用启用观察，PPPoE 拨号连接尝试重新创建，再次确认拨号用户名密码输入正确，观察上网是否正常，此部分还可尝试替换不同 PC 连接观察。

(7) 检查是否上网慢

确认客户 PC 打开各类门户网站是否比正常使用时明显缓慢，下载速度是否很低。

(8) 检查宽带问题

通过网管软件或者流量监控软件监控上层 OLT 等设备的接口带宽，确认流量是否已经接近接口带宽值或设备吞吐量，如果出现此情况，需要通过扩容增加带宽。

(9) 检查 Cable 网络下行广播流量

在 OLT 口或者支持镜像的头端以太网口镜像抓包(镜像具体配置参加产品手册)，确认网络中存在如下两种现象，则需要特别引起注意，并通过优化汇聚设备(如 OLT 等)的配置和组网，包括端口隔离、缩小广播域(建议采用 PSPUPV 方式组网，每 OLT 一个管理 VLAN)的方式减少网络中的广播流量。

① 广播流量大于 5Mbps 以上。

② 存在大量源 MAC 连续的广播包。

(10) 检查 Cable 线路噪声

① 同轴网检查建议。

(a) 查看广电机箱内，各设备、分支器、分配器等的 Cable 口是否连接紧密，是否存在 Cable 接口松动，屏蔽层和内芯铜线是否有搭接或屏蔽层和固定头是否未接触(这样就起不到屏蔽的作用)，建议可以对部分不好的接头重新制作。另外，光机、头端、机箱等必须按要求严格接地。

(b) 同轴网线路必须严格按照《H3C EPCN 工程安装指导》的要求进行工程实施，如存在放大器，则需要对 EoC 信号覆盖的所有放大器使用低通旁路器进行跨接，或对放大器内部做改造。

(c) 入户线路需注意线路是否存在破损，是否和多根电源线捆绑，设备位置周边是否摆放有高功率家用电器等，都会产生噪声干扰，需要重做线路或者移除干扰源观察。

② 噪声解决建议。

增强 EoC 信号强度。

(a) 光节点下移，通过将光节点下移到楼道，减少野外分支分配网中噪声干扰，拉近头端到终端的距离。

(b) 增加光节点下头端数量，用一路头端带一个混合器，提高头端和终端接收信号强度。

(c) 尽量采取星型分配组网，串接分支器尽量少，减少树形组网中分支器的衰减。

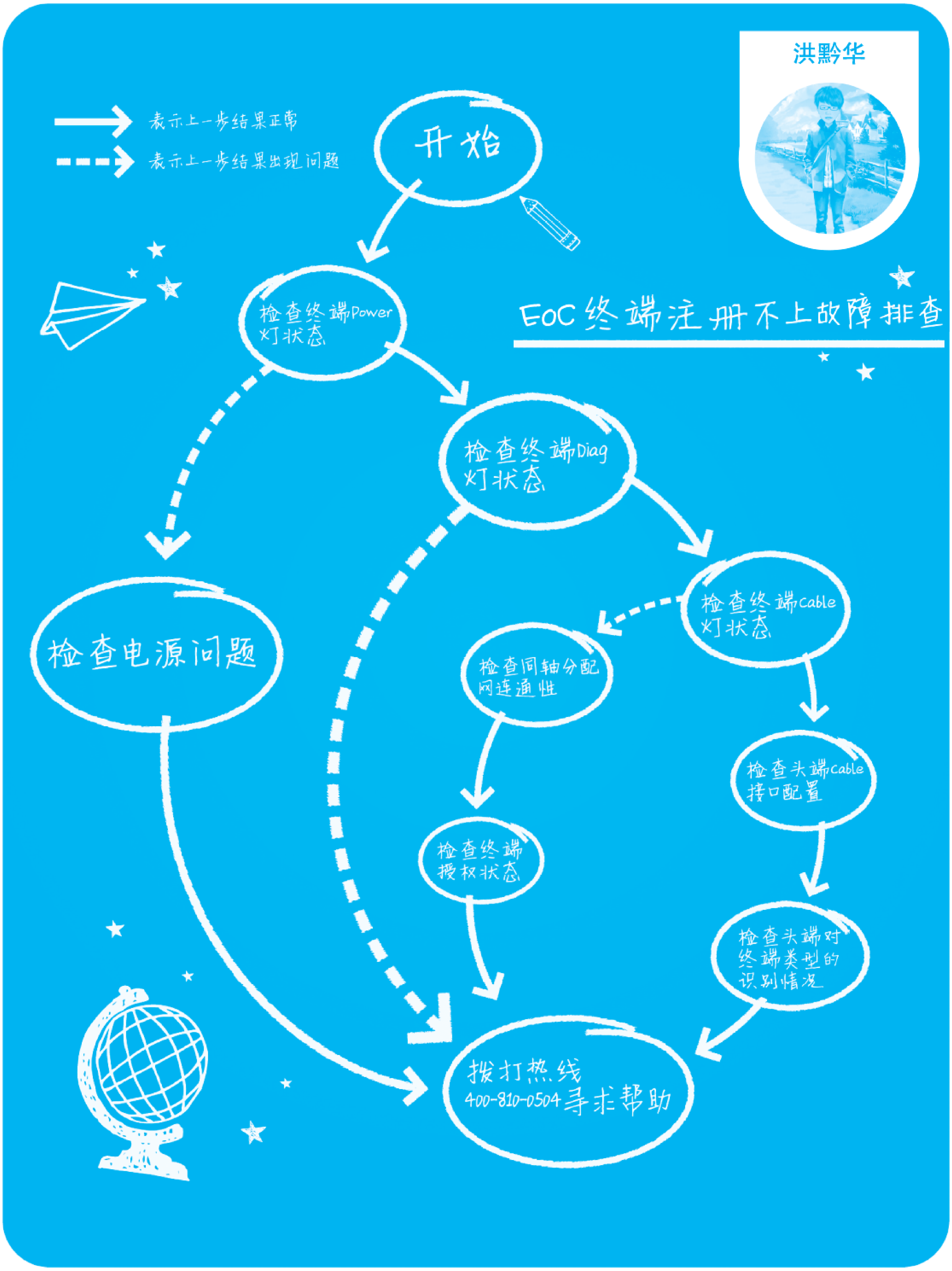
(d) 减少 EoC 用户同轴分配网中分支分配器和接头的数量，减少 EoC 信号的插入损耗。

屏蔽噪声源。

(a) 运用频谱仪、场强仪、手持式 EPCN 测试仪等、手持我司终端(电源可用干电池制作出 DC 9V 的电源)等方式分段排查，找到噪声源并对噪声源采用高通滤波器过滤。

(b) 在 iMC 或头端上查看终端上下行速率，当衰减正常时，上下行速率有异常，可判断噪声源离此终端较近，可从此终端处分配器开始往上排查。

(c) 用户处连接不建议通过二分配连接终端和电视；建议按照 Cable 口连接用户总进线，TV 口接用户电视机；通过内部的高通模块防止 TV 口噪声漏出到主线路上影响其他终端；用户处终端接线完成后，不仅需要测试用户上网速率，还应检查用户处电视节目是否正常。


洪黔华
EoC 终端注册不上故障排查
表示上一步结果正常
表示上一步结果出现问题
开始
检查终端Power灯状态
检查终端Diag灯状态
检查电源问题
检查终端Cable灯状态
检查同轴分配网连通性
检查头端Cable接口配置
检查终端授权状态
检查头端对终端类型的识别情况
拨打热线
400-810-0504寻求帮助

1. 开始

EPCN 终端注册不上问题的原因包含硬件、Cable 网络、软件配置等，所以定位故障的思路是：首先观察终端各指示灯状态、配合替换法逐步排查，然后检查同轴网络的连通性，最后再检查头端的特殊配置。

2. 流程图相关操作说明

(1) 检查终端 Power 灯状态

终端的 Power 灯正常情况下处于常亮状态，如果不是说明电源适配器输出问题或者终端故障。

(2) 检查电源问题

① 检查终端电源接口是否插紧，是否正常连接。

② 检查插线板或者插座是否已经通电，可接上其他电器设备测试验证。

③ 检查插线板或者插座与终端电源适配器接触是否良好。

④ 更换一个相同型号的终端电源适配器观察是否正常。

(3) 检查终端 Diag 灯状态

终端上电后，Diag 灯正常情况下处于熄灭状态。

① 如果亮一会后自动熄灭，说明系统正在自检、软件正在自动更新或者 Cable 链路正在自检，属于正常情况。

② 如果一直常亮或者闪烁，均表示终端故障，建议更换终端观察。

(4) 检查终端 Cable 灯状态

终端的 Cable 灯正常情况下处于常亮状态。

① 如果是一亮一灭交替闪烁，表示终端正在与头端建立连接。

② 如果常亮则表示终端与头端之间链路已正常建立，需要查看头端软件配置是否正确。

③ 如果不亮则说明 Cable 链路未建立连接，可能是线路不通、链路衰减过大或终端未被授权。

(5) 检查同轴分配网连通性

① 在终端处使用频谱分析仪或者扫频仪测试 7.5～65MHz 频段是否有接收到头端发出的 EOC 信号，或者使用信号发生器和场强仪测试 Cable 网络传输 7.5～65MHz 的低频段是否正常。

② 使用频谱分析仪或场强仪测试头端所在光节点处第一个频道所处电视频点的接收功率，减去在终端处测试相同频点所得的接收功率值，得出 Cable 网络衰减大小，检查是否符合双向网改造要求(推荐值 20～50dB)，是否符合 Cable 网络设计要求，如果衰减太大或与设计不符，需要调整 Cable 网络中的分支分配器、重做 Cable 线路接头、下移光节点等方式解决。

(6) 检查终端授权状态

① 进入头端设备管理界面→“Cable 管理”→“网络拓扑”，正常情况下在线终端的链路状态显示为✓；确认终端 MAC 对应的链路状态是否为 ×，说明该终端与头端当前未正常建立连接，如图 10-18 所示。

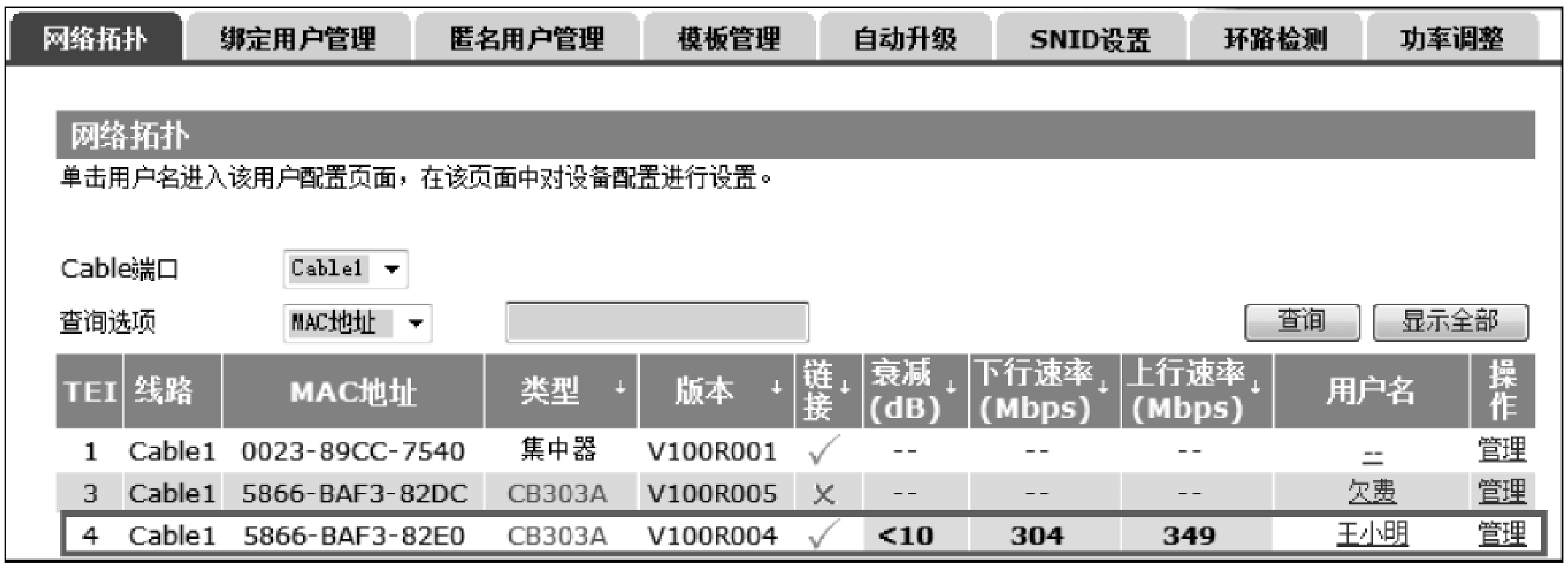


图 10-18 终端 MAC 对应的链路状态

② 选择“Cable 管理”→“绑定用户管理”，查看终端是否被管理员配置为禁止接入了。如果该终端需要被授权，选中 MAC 地址前面的复选框后单击“允许”按钮，对该终端进行授权配置，如图 10-19 所示。

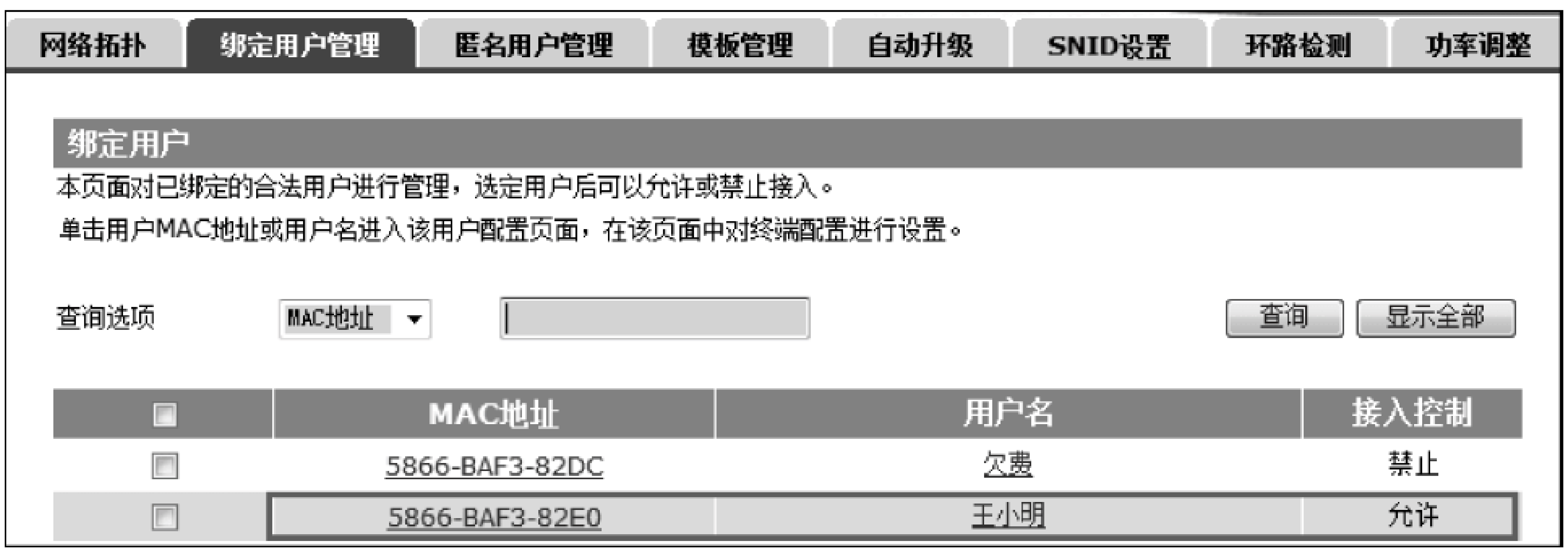


图 10-19 对终端进行授权配置

(7) 检查头端 Cable 接口配置

① 进入头端设备管理界面→“Cable 管理”→“网络拓扑”，查看页面是否提示未发现网络拓扑，如图 10-20 所示。

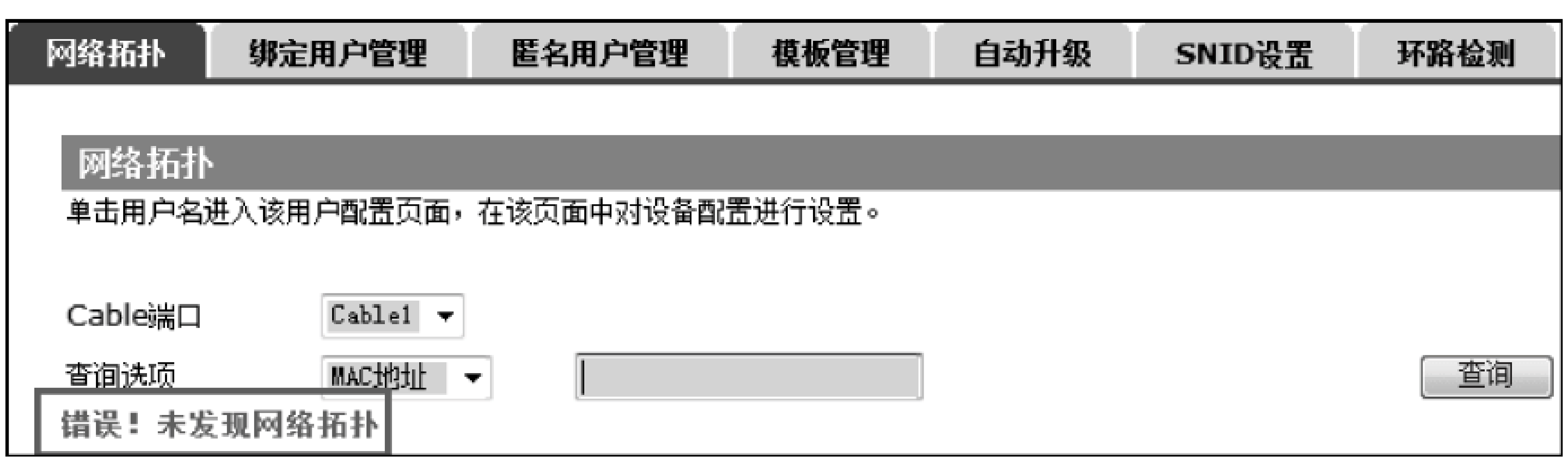
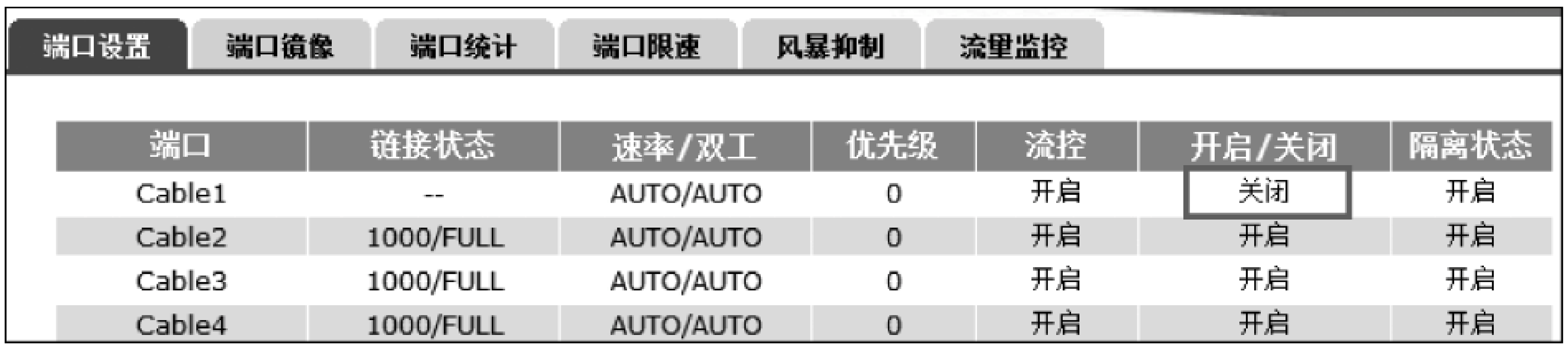


图 10-20 未发现网络拓扑提示

② 进入头端 Web 管理界面→“端口管理”→“端口设置”，查看 Cable 端口状态，如果为关闭状态，需要将其打开，如图 10-21 所示。

(8) 检查头端对终端类型的识别情况

① 进入头端 Web 管理界面→“Cable 网络拓扑”，正常情况下头端能够显示该终端的具体型号，如 CB303A，查看终端的类型是否无法正确显示或者显示为红色，说明该终端未被头端



端口	链接状态	速率/双工	优先级	流控	开启/关闭	隔离状态
Cable1	--	AUTO/AUTO	0	开启	关闭	开启
Cable2	1000/FULL	AUTO/AUTO	0	开启	开启	开启
Cable3	1000/FULL	AUTO/AUTO	0	开启	开启	开启
Cable4	1000/FULL	AUTO/AUTO	0	开启	开启	开启

图 10-21　Cable 端口状态

正常识别，无法正常开展业务，如图 10-22 所示。



TEI	线路	MAC地址	类型	版本	链接	衰减(dB)	下行速率(Mbps)	上行速率(Mbps)	用户名	操作
1	Cable1	5866-BAF3-C8AF	集中器	V100R002	√	--	--	--	--	管理
3	Cable1	DC02-8EAA-E0F0	--	5-1-5100	√	--	--	--	--	管理

图 10-22　Cable 端口类型

② 检查终端类型管理列表，确认是否已经添加了该终端类型，如图 10-23 所示。



终端HFID	终端类型	端口数量	交换芯片类型	端口映射(端口-phy)	厂商信息
CNU302-A	网桥型	2	RTL8306	1-0, 2-1	H3C-HP
CNU303-A	网桥型	3	RTL8306	1-0, 2-1, 3-2	H3C-HP
CNU304-A	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	H3C-HP
D101	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CISCO
CT1000-402	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	DATANG
C104NU	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CHULING
HMD404T	网桥型	4	AR8236	1-2, 2-3, 3-4, 4-5	B-STAR
HMD403T	网桥型	3	AR8236	1-2, 2-3, 3-4	B-STAR
HG7042T	网桥型	4	RTL8306	1-3, 2-2, 3-1, 4-0	HUAWEI
YT7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	YITONG
GSD7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	GAOSHIDA

图 10-23　终端类型管理列表

③ 如果终端是非 H3C 设备，需要先升级头端至支持与友商互联互通的版本，具体版本请联系 H3C 呼叫中心寻求帮助，然后在终端类型管理页面单击“新建”进入“终端类型信息”配置页面，部分参数如终端 HFID、交换芯片类型、端口映射关系等需要联系终端厂家获取并如实填入，如图 10-24 所示。

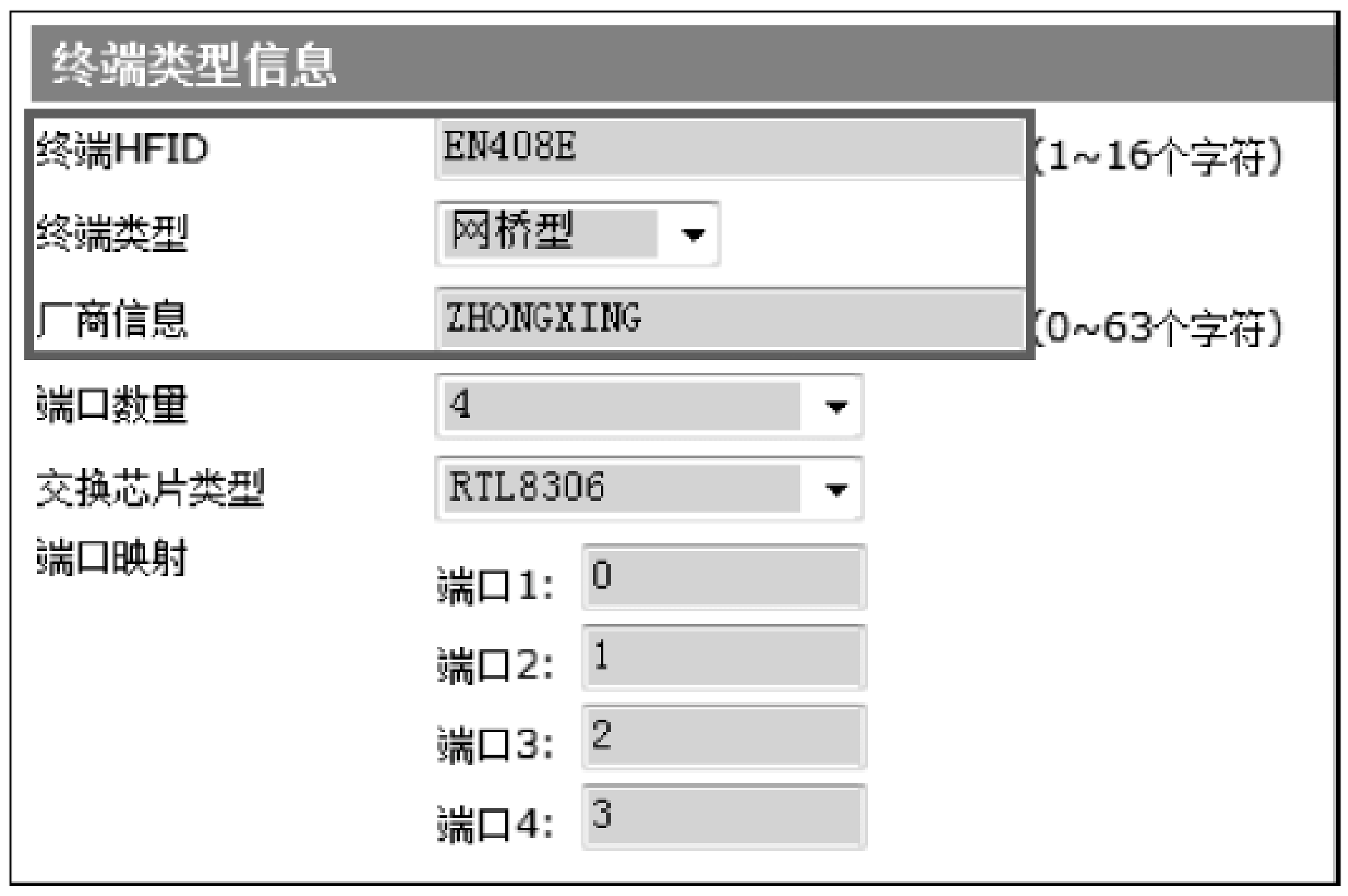


图 10-24　终端类型信息

成功添加以后如图 10-25 所示。



	终端HFID	终端类型	端口数量	交换芯片类型	端口映射(端口-phy)	厂商信息
	CNU302-A	网桥型	2	RTL8306	1-0, 2-1	H3C-HP
	CNU303-A	网桥型	3	RTL8306	1-0, 2-1, 3-2	H3C-HP
	CNU304-A	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	H3C-HP
	D101	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CISCO
	CT1000-402	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	DATANG
	C104NU	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CHULING
	HMD404T	网桥型	4	AR8236	1-2, 2-3, 3-4, 4-5	B-STAR
	HMD403T	网桥型	3	AR8236	1-2, 2-3, 3-4	B-STAR
	HG7042T	网桥型	4	RTL8306	1-3, 2-2, 3-1, 4-0	HUAWEI
	YT7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	YITONG
	GSD7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	GAOSHIDA
	EN408E	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	ZHONGXING

图 10-25　终端类型管理

EoC终端配置下发不生效故障排查

洪黔华



1. 开始

EPCN 是 H3C 针对广电接入网双向改造推出的技术，是低频 EoC 技术的一种，通过广播电视同轴网共缆传输电视信号和 EoC 数据信号。EoC 终端配置下发不生效问题位故障的思路是：首先判断是否为我司终端，如果是非我司终端，头端版本是否升级到支持互联互通特性的版本，是否已经添加了此新终端类型，然后再检查终端配置是否正确，检查同轴线路质量，最后再替换终端观察。

2. 流程图相关操作说明

(1) 检查终端是否为我司设备

检查当前配置下发不成功的终端是否为我司设备。

(2) 检查头端版本支持互联互通

① 进入头端设备 Web 管理界面→“Cable 管理”，如果有如图 10-26 所示“终端类型管理”设置页面，则当前版本已经支持互联互通特性，如果没有，则需要升级版本。



图 10-26 “终端类型管理”页面

② 表 10-3 所示为我司主要头端开始支持互联互通特性的版本号，升级至以下版本及以后的版本都支持互联互通特性，不在列表中的头端请咨询呼叫中心确认！

表 10-3 支持互联互通特性的版本

头端型号	版　　本	头端型号	版　　本
CC600E	暂无	CC754	CC754E01106
CC620E	暂无	CC710E	CC710E01103
CC700E	CC700EV100R005	CC712E	CC712E01103
CC720E	CC720EV100R007	CC721E	CC712E01103

③ 进入头端设备 Web 管理界面→"系统管理"→"软件升级",单击页面上的链接,如图 10-27 所示,登录 H3C 公司网站下载最新的软件版本,保存到本地计算机。

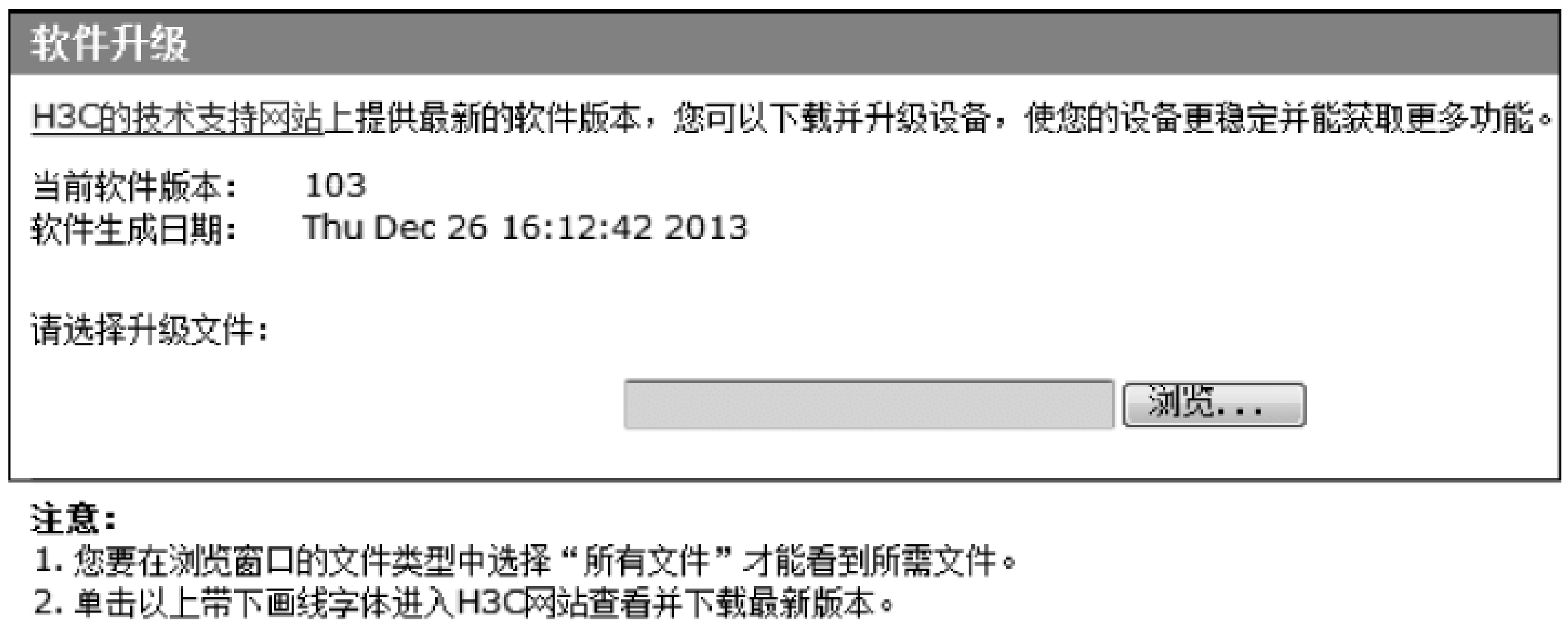


图 10-27 下载最新的软件版本

④ 单击"浏览..."按钮在本机上选择该升级版本文件,单击页面上的"确定"按钮开始升级。完成升级后,设备会自动重启。

⑤ 对于二合一头端,也可以选择将版本上传到我司 OLT,通过 OLT 批量升级。

(3) 检查头端是否默认支持该终端类型

进入头端设备 Web 管理界面→"Cable 管理"→"终端类型管理",如图 10-28 所示,根据 HFID(需要咨询终端厂家获取,一般为终端型号)查看终端类型默认支持列表中是否已存在配置下发不生效的终端类型。

☐	终端HFID	终端类型	端口数量	交换芯片类型	端口映射	厂商信息
☐	D101	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	LAKETUNE
☐	EN408E	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	ZTE
☐	CT1000-402	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	DATANG
☐	C104NU	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CHULING
☐	HMD404T	网桥型	4	AR8236	1-2, 2-3, 3-4, 4-5	B-STAR
☐	HMD403T	网桥型	3	AR8236	1-2, 2-3, 3-4	B-STAR
☐	HMD404	网桥型	4	AR8236	1-2, 2-3, 3-4, 4-5	B-STAR
☐	HMD403	网桥型	3	88E6061	1-0, 2-4, 3-1	B-STAR
☐	HMD402	网桥型	2	88E6031	1-0, 2-4	B-STAR
☐	HG7042T	网桥型	4	RTL8306	1-3, 2-2, 3-1, 4-0	HUAWEI
☐	YT7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	YITONG
☐	GSD7411	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	GAOSHIDA
☐	E330	网桥型	2	RTL8306	1-0, 2-1	CISCO
☐	E330.2	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	CISCO
☐	PT1Q115	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	SVA
☐	T52X4E-O	网桥型	4	RTL8306	1-3, 2-2, 3-1, 4-0	YUNSHI
☐	ECM201	网桥型	1	_	_	--
☐	C214NU	网桥型	4	RTL8306	1-0, 2-1, 3-2, 4-3	HUAGUANG
☐	HG-AU204	网桥型	4	RTL8306	1-3, 2-2, 3-1, 4-0	HUAGUANG

图 10-28 终端类型管理

(4) 确认终端符合互联互通对接要求

我司头端互联互通特性支持的终端需要符合如下要求。

① 终端 EoC 芯片需要为 Intellon 6400 系列或 AR7400 系列芯片。

② 只支持一个以太网口的友商终端,或者支持多个以太网口的终端,但所使用的交换芯片需为 RTL8306、AR8236、88E6061、88E6031 中的一种。

③ 友商终端为网桥型终端，网关型终端待后续版本支持，请关注 H3C 官方网站的正式版本发布情况及其说明书。

(5) 添加新终端类型参数

进入头端设备 Web 管理界面→“Cable 管理”→“终端类型管理”，单击“新建”按钮，逐项添加配置项，完成后单击“确认”按钮并保存头端配置。对于 HFID、终端类型、交换芯片类型、端口映射关系参数均需要终端厂商提供，请确认后填入，否则可能出现配置下发不生效的问题。

例如，华为的某个终端 HFID 为 HG7042T，终端类型为网桥型，以太网端口数为 4 个，交换芯片类型为 RTL8306，端口映射关系为端口 1 对应交换芯片接口 3，端口 2 对应交换芯片接口 2，端口 3 对应交换芯片接口 1，端口 4 对应交换芯片接口 0；配置如图 10-29 所示。

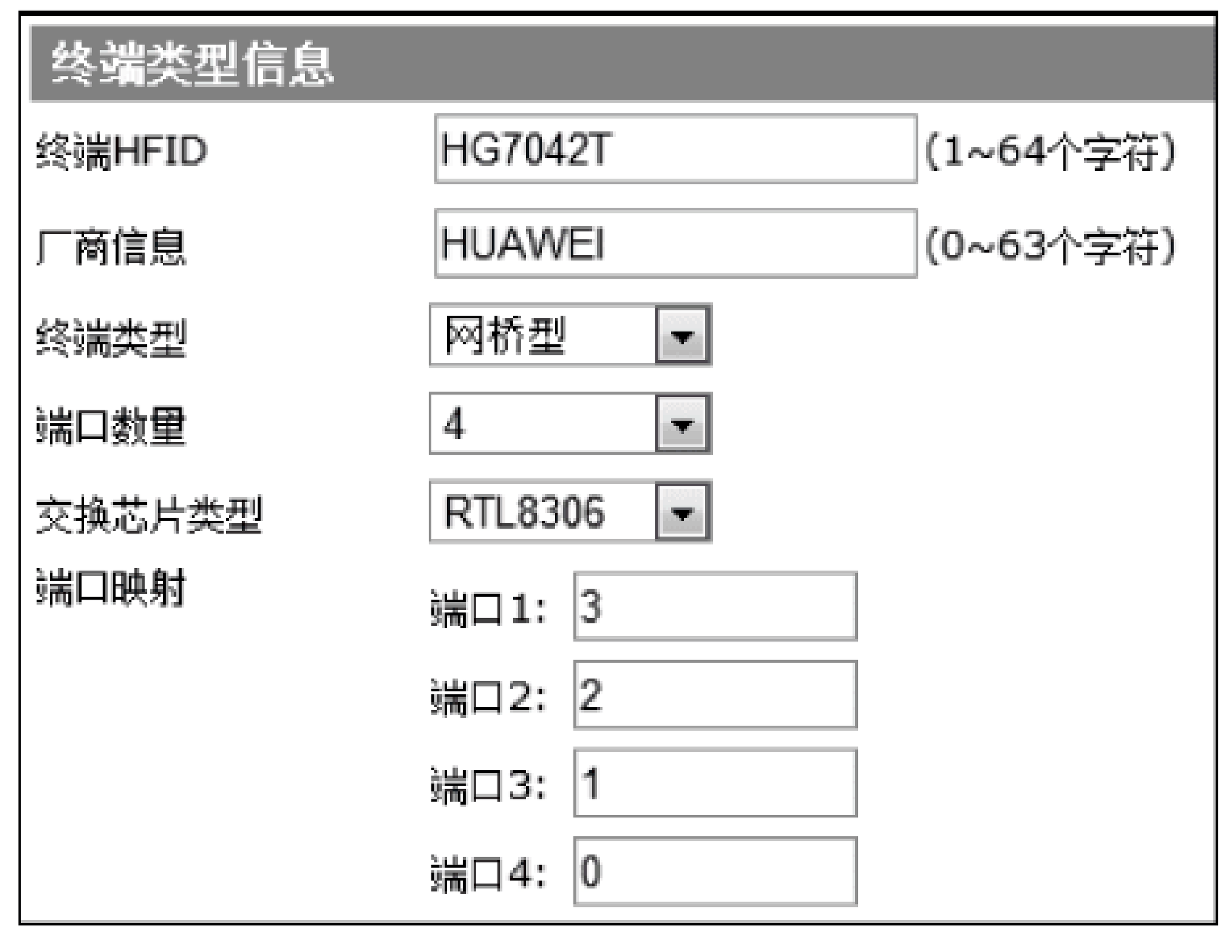


图 10-29　终端类型信息

(6) 检查配置正确性

进入头端设备 Web 管理界面→“高级管理”→“LOG 设置”→“日志信息”，查看头端日志，是否存在配置下发成功或者失败的告警。

```
UPDATE_CFG: The switch configuration of CNU (5866-baf3-82e0) was updated successfully.
UPDATE_CFG: The switch configuration of CNU (5866-baf3-82e0) was updatedfailed.
```

① 如果提示终端配置下发成功，但配置未按要求生效，即上网或者 IP TV 还是不通，则按如下步骤检查。

(a) 检查终端类型管理中的端口映射顺序配置是否填反，端口数量是否填错。

(b) 检查终端模板配置是否按规划填入，MAC 地址个数限制是否为默认配置。

(c) 检查终端是否错误绑定了其他模板。

(d) 检查头端 VLAN 配置，如果是 802.1Q VLAN 模式，确认头端是否创建了业务 VLAN，上行口是否允许业务 VLAN 通过。

(e) 检查头端接口和物理线路连接是否存在问题。

② 如果提示终端配置下发失败或终端接入后长时间无此提示，则按如下步骤检查。

(a) 检查终端类型管理中的终端类型配置是否选错，终端交换芯片型号当前头端版本是否支持，通过查看终端类型管理配置中的交换芯片选项可确认，不在下拉框中即为不支持的型号。

(b) 检查终端连接状态当前是否处于“×”离线状态。

(c) 检查终端是否存在环路，可开启头端环路检测确认。

(d) 检查终端版本是否与头端版本配套，配套关系参见头端版本说明书，头端无法显示终端版本号等终端注册不上问题参见另一云图《EoC 终端注册不上故障排查》。

(e) 如果是通过网管下发，通过 ping 头端管理地址检查链路连通性，并检查头端的 SNMP 配置是否正确。

(7) 检查同轴线路质量

① 同轴网检查步骤。

第一，检查头端是否存在线路质量告警信息。

(a) 进入头端设备 Web 管理界面→“高级管理”→“LOG 设置”→“日志信息”，查看头端日志，是否存在上下行速率较大波动的告警，说明同轴线路存在噪声等干扰。

```
%Jan  6 04:57:16 1970 H3C ACMP/3/TX_RATE_ERR: The TX rate drop of CNU (3822-d6c2-d61e) turns into 95, which is under the minimal threshold(50).
%Jan  6 04:57:16 1970 H3C ACMP/3/RX_RATE_ERR: The RX rate drop of CNU (3822-d6c2-d61e) turns into 65, which is under the minimal threshold(50).
```

(b) 进入头端设备 Web 管理界面→“Cable 管理”→“网络拓扑”，不断刷新 Cable 状态查看终端上下行速率和终端衰减，是否存在低于告警门限值，状态为黄、红色特别是红色的情况，如图 10-30 所示。当衰减正常时，上下行速率有异常，可判断噪声源离此终端较近，可从此终端处分配器开始往上级排查。

链接	衰减(dB)	下行速率(Mbps)	上行速率(Mbps)
✓	--	--	--
✓	--	--	--
✓	52	147	75
✓	--	--	--
✓	--	--	--
✓	55	149	87
✓	--	--	--
✓	54	118	93
✓	47	143	148
✓	42	148	108
✓	46	123	63
✓	49	147	50
✓	53	112	108
✓	45	146	145
✓	--	--	--

图 10-30 上下行速率和终端衰减情况

最佳情况参考如表 10-4 所示。

表 10-4 头端＋终端组网最佳情况

头端＋终端组网情况	衰减(dB)	上下行速率(Mbps)
CC6XX 头端＋CB2XX 终端	>10,<60	>100,<160
CC6XX 头端＋CB3XX 终端	>10,<60	>100,<160
CC7XX 头端＋CB2XX 终端	>10,<55	>100,<160
CC7XX 头端＋CB3XX 终端	>10,<55	>400,<460

(c) 进入头端设备 Web 管理界面→“Cable 管理”→单击终端列表中的“管理”链接→“链路状态”，目标方向选择一个终端 MAC 地址，单击“获取信息”按钮，查看该终端与头端之前的链路质量情况，重点关注平均 Pre-FEC 比特错误率(正常值小于 10%)、平均 Bits/Carrier(正常值范围在 4～10)、平均 SNR/Carrier 参数(正常值大于 15dB，小于 30dB 时，该信道的传输效率就能达到满效率传输)。详细参数说明请参考各产品的《×××产品用户手册》，截图如图 10-31 所示。



图 10-31 终端与头端之前的链路质量情况

第二，同轴网线路必须严格按照《H3C EPCN 工程安装指导》的要求检查工程实施质量，如存在放大器，则需要对 EoC 信号覆盖的所有放大器使用低通旁路器进行跨接，或对放大器内部做改造。

第三，查看广电机箱内，各设备、分支器、分配器等的 Cable 口是否连接紧密，是否存在 Cable 接口松动，屏蔽层和内芯铜线是否有搭接或屏蔽层和固定头是否未接触(这样就起不到屏蔽的作用)，建议可以对部分不好的接头重新制作。另外，检查光机、头端、机箱等是否已按要求严格接地。

第四，查看线路排布，检查线路是否有破损，是否与多根电源线捆绑，同时观察走线是否存在可见的强干扰源(类似于高压线、变电站等)，用户侧还需要检查设备位置周边是否摆放有高功率家用电器等。确认现场走线不存在强干扰源。

第五，运用可测试低频信号的频谱仪、场强仪、手持式 EPCN 测试仪等，或手持我司终端(电源可用干电池制作出 DC 9V 的电源)等方式分级排查，上行速率低就从终端入户线路开始测试，下行速率低就从头端光节点处开始，断开各分支分配器上的 Cable 口，测试线路上低频段 1～86MHz 的噪声情况，线路底噪需要小于 35dB。

如图 10-32 所示，线路中存在全频段噪声干扰，需要逐级确认并排除噪声源，详细排查步骤可参考《H3C 广电 EPCN 噪声排查指导书 V1.1.docx》。

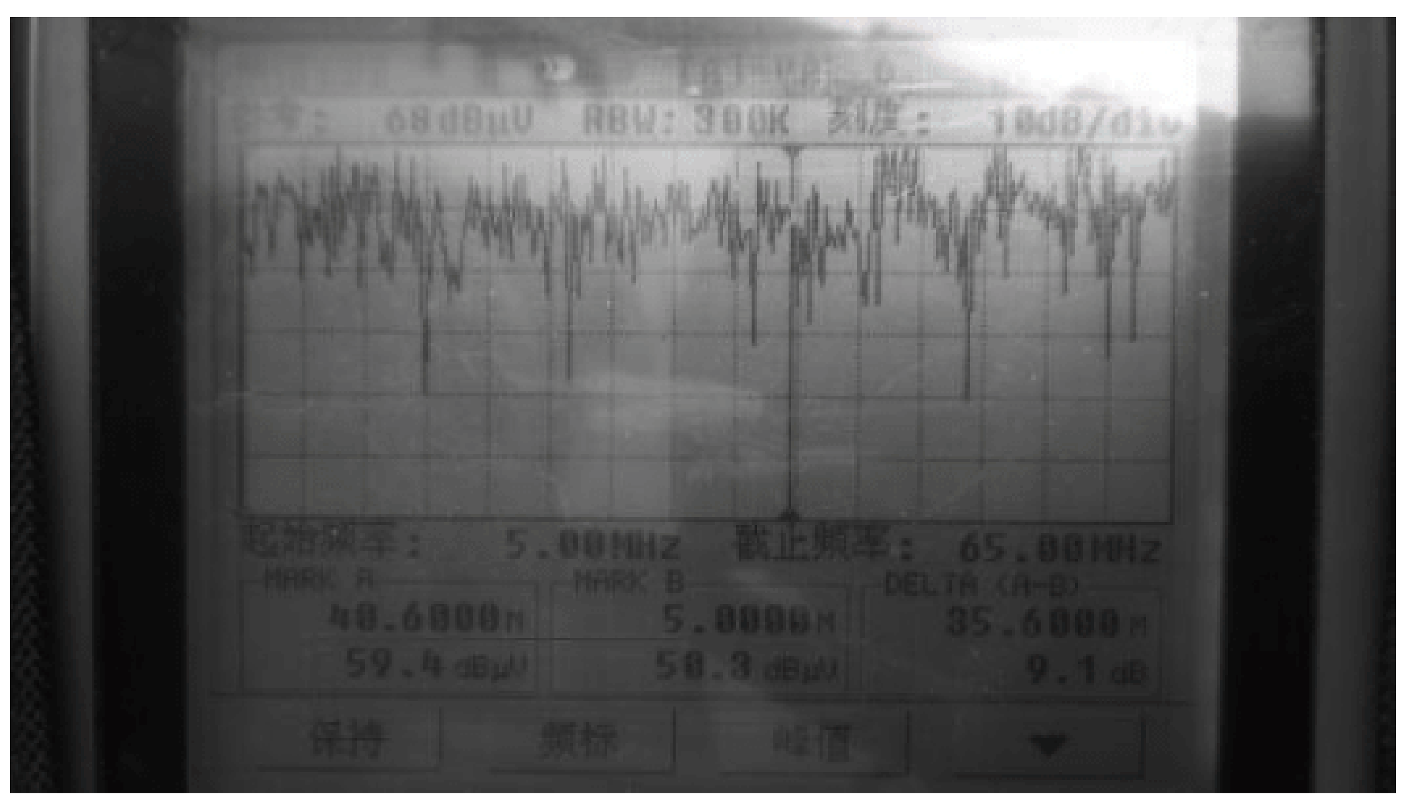


图 10-32 全频段噪声干扰

② 噪声解决建议。

(a) 增强 EoC 信号强度。

第一，光节点下移，通过将光节点下移到楼道，减少野外分支分配网中噪声干扰，拉近头端到终端的距离。

第二，增加光节点下头端数量，用一路头端带一个混合器，提高头端和终端接收信号强度。

第三，尽量采取星形分配组网，串接分支器尽量少，减少树形组网中分支器的衰减。

第四，减少 EoC 用户同轴分配网中分支分配器和接头的数量，减少 EoC 信号的插入损耗。

(b) 屏蔽噪声源。

第一，对噪声源采用高通滤波器过滤。

第二，移除或避开怀疑的干扰源如强功率电器、变电站等。

第三，Cable 线缆与电源走线隔离开。

第四，光机、头端、机箱等按要求严格接地。

第五，用户处连接不建议通过二分配连接终端和电视；建议按照 Cable 口连接用户总进线，TV 口接用户电视机；通过内部的高通模块防止 TV 口噪声漏出到主线路上影响其他终

端；用户处终端接线完成后，不仅需要测试用户上网速率，还应检查用户处电视节目是否正常。

(8) 替换终端观察

① 如果经过上述步骤排查故障依旧，可尝试更换一个新终端观察，排除终端单台故障原因。

② 如果依旧无法解决，请参考《H3C EPCN 产品一般故障信息收集方法. pdf》准备好头端诊断信息、配置、日志、上述步骤排查时收集的信息和详细故障描述，拨打 H3C 呼叫中心热线电话寻求帮助。

后　　记

伴随着时代的快速发展，IT技术已经与人们的日常生活密不可分，在越来越多的人依托网络进行沟通的同时，IT技术本身也演变成了服务、需求的创造和消费平台，这种新的平台逐渐创造了一种新的生产力，一股新的力量。

新华三集团（简称新华三）是全球领先的新IT解决方案领导者，致力于新IT解决方案和产品的研发、生产、咨询、销售及服务。以技术创新为核心引擎，新华三50%的员工为研发人员，专利申请总量超过6 800件，其中90%以上是发明专利。2015年新华三申请专利841件，平均每个工作日超过3件。

为了使广大网络产品使用者和网络技术爱好者能够更好地掌握新华三相关产品技术，新华三集团相关部门人员开发了大量的技术资料，详细地介绍了相关知识。这些技术资料大部分是公开的，在新华三集团的官方网站（http://www.h3c.com/cn/）上都能看到并下载。

但是，在传统的纸质媒介仍占重要地位的今天，许多合作伙伴和学校、机构、网络技术爱好者都希望新华三集团能够正式出版其技术资料，包括网络学院教材、产品配置手册、典型配置案例、行业解决方案等。作为国内IT领域技术和设备制造的领导者，新华三集团深感自身责任重大，责无旁贷。

2004年10月份，新华三集团的前身——杭州华三通信技术有限公司（简称华三）出版了自己的第一本网络学院教材，开创了业界相关培训教材正式出版的先河，极大地推动了IT技术在业界的普及。在后续的几年间，华三公司陆续出版了《IPv6技术》（第二版）、《路由交换技术第1卷》、《路由交换技术第2卷》、《路由交换技术第3卷》、《路由交换技术第4卷》等网络学院教材系列书籍，以及《H3C以太网交换机典型配置指导》、《H3C路由器典型配置指导》等网络学院参考书系列书籍，极大的推动了IT技术在网络学院和网络技术业界的普及。

《根叔的云图——网络故障大排查》是新华三集团所推出的网络学院教材中的重要一本，其集中了新华三集团内上百位专家十多年工作的经验，开创了类似书籍的先河。

新华三集团希望通过这种形式，探索出一条理论和实践相结合的教育方法，顺应国家提倡的“学以致用、工学结合”教育方向，培养更多实用型的IT技术人员。

希望在IT技术领域，这一系列教材能成为一股新的力量，回馈广大IT技术爱好者，为推进中国IT技术发展尽绵薄之力，同时也希望读者对我们提出宝贵的意见。

新华三大学培训开发委员会

2016年11月